

Unit A3

Mathematical language and proof

Introduction

This unit gives an introduction to mathematical proof. While you have already met proofs in your previous mathematical studies, the emphasis of your studies is likely to have been not on proofs, but on problems that can be solved by, essentially, *computing* a result.

In this module the emphasis shifts to a more abstract approach to mathematics, where the goal is to describe clearly properties of mathematical objects using mathematical statements, and to establish their correctness using proofs.

Section 1 introduces the language used to express mathematical statements and reviews the ways in which statements can be combined. Sections 2 and 3 introduce various techniques for proving that a mathematical statement is true. As a further introduction to abstract mathematical thinking, Section 4 introduces the concept of an *equivalence relation* on a set. Equivalence relations are important in many areas of mathematics. You will meet them again in the group theory units of this module.

1 Mathematical statements

In Units A1 *Sets, functions and vectors* and A2 *Number systems* you have seen many examples of mathematical statements, theorems and proofs. In this section you will look in detail at mathematical statements and the ways in which they can be combined and negated. This sets the scene for Sections 2 and 3, where you will learn about methods of proof.

1.1 Statements and negations

The building blocks of mathematical theorems and proofs are assertions called **statements**, also known as **propositions**. In mathematics, a statement is an assertion that is either true or false, though we may not know which. The following are examples of statements.

1. The equation $2x - 3 = 0$ has solution $x = \frac{3}{2}$.
2. $1 + 1 = 3$.
3. $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ for each positive integer n .
4. There is a real number x such that $\cos x = x$.
5. Every even integer greater than 2 is the sum of two prime numbers.
6. x is greater than 0.

In this list, Statement 1 is true and Statement 2 is false. Statements 3 and 4 are both true, though this is probably not immediately obvious to you in either case. We shall prove that Statement 3 is true later in this section. You can check that Statement 4 is true by noting that the graphs of $y = \cos x$ and $y = x$ intersect; a rigorous proof can be obtained by using the *Intermediate Value Theorem*, which you will meet in the analysis units of this module. At the time of writing it is not known whether Statement 5 is true or false; it is known as *Goldbach's Conjecture*, and mathematicians have been trying to prove it since 1742.



Figure 1 Extract from Goldbach's letter to Euler

On 7 June 1742 the German mathematician Christian Goldbach (1690–1764) posed his conjecture in a letter to Leonhard Euler (1707–1783). An extract from this letter is shown in Figure 1. In the same letter Goldbach also proposed what is now known as the *Weak Goldbach Conjecture*. This states that every odd number greater than 5 can be expressed as the sum of three primes. The Weak Goldbach Conjecture was proved by the Peruvian mathematician Harald Helfgott in 2013. Goldbach and Euler first met at the St Petersburg Academy of Sciences in 1727 when Euler was appointed to a position in the mathematics division, and where Goldbach was professor of mathematics. After Goldbach moved to Moscow in 1729 they began a correspondence which lasted 35 years.

Statement 6 is a little different from the others, since whether it is true or false depends on the value of the variable x . A statement, such as this one, that is either true or false depending on the value of one or more variables, is called a **variable proposition**. We usually denote statements by the capital letters P, Q, R, \dots , and we denote variable propositions containing the variable x by $P(x), Q(x), \dots$.

When considering a variable proposition, we must have in mind a suitable set of values from which the possible values of the variable are taken. For example, the set associated with Statement 6 might be \mathbb{R} , since for each real number x the assertion is either true or false. A variable proposition with several variables may have several such associated sets. Often the set or sets associated with a variable are clear from the context and so we do not state them explicitly. In particular, unless it is stated otherwise, we assume that if the variable is x or y , then the associated set is \mathbb{R} , whereas if the variable is n or m , then the associated set is \mathbb{Z} or \mathbb{N} , depending on the context.

An example of an assertion that is not a mathematical statement is ‘ $\{1, 2\}$ is greater than 0’. Since $\{1, 2\}$ is a set, and sets cannot be greater than (nor less than or equal to) zero, the assertion is meaningless, and therefore is neither true nor false. Other examples are ‘ π is interesting’ and ‘1000 is a large number’, which are not precise enough to be either true or false.

Exercise A101

Determine whether each of the following assertions is a mathematical statement. For those that are mathematical statements, state whether or not they are variable propositions.

- (a) n is even or n is prime.
 - (b) The set of odd integers less than 3 is small.
 - (c) $\{1, 2, 3, 4\}$ is odd.
 - (d) $\{1, 2, 3, 4\} \cap \{6, 7, 8, 9\} \neq \emptyset$.
- (Remember that \emptyset denotes the empty set.)

A **theorem** is simply a mathematical statement that is true. However, we usually reserve the word for a statement that is considered to be of some importance, and whose truth is not immediately obvious, but instead has to be proved. A **proposition** is a ‘less important’ theorem, and a **lemma** is a theorem that is used in the proof of other theorems. A **corollary** is a theorem that follows from another theorem by a short additional argument. Theorems are sometimes called *results*.

As you may have noticed, we have used the word *proposition* in two quite different ways in this subsection. It can either mean a ‘less important’ theorem, as just explained, or it can be used with the same meaning as the word ‘statement’ (this is its meaning in the phrase ‘variable proposition’). Both meanings are in common use in mathematics, so you should be aware of them both. Normally, the intended meaning will be clear from the context.

Every statement has a related statement, called its **negation**, which is true when the original statement is false, and false when the original statement is true. The negation of a statement P can usually be written as ‘it is not the case that P ’, but there are often better, more concise ways to express a negation. Thus, for example, the negation of the variable proposition

x is greater than 0

can be written as

it is not the case that x is greater than 0,

but is better expressed as

x is not greater than 0

or even as

$x \leq 0$.

We usually denote the negation of a statement P by ‘not P ’. The process of finding the negation of a statement is called **negating** the statement. Here are some more examples.

Worked Exercise A45

Express concisely the negations of each of the following statements.

- (a) There are at least 10 two-digit natural numbers less than 20.
- (b) π is less than 5.

Solution

- (a) The negation can be expressed as

There are at most 9 two-digit natural numbers less than 20,

or as

There are fewer than 10 two-digit natural numbers less than 20.

- (b) The negation can be expressed as

π is greater than or equal to 5,

or as

$\pi \geq 5$.

Exercise A102

Express concisely the negations of each of the following statements.

- (a) $x = \frac{3}{5}$ is a solution of the equation $3x + 5 = 0$.
- (b) The equation $n^2 + n - 2 = 0$ has exactly two solutions.

In the rest of this section you will learn about the possible structures of mathematical statements and their negations.

1.2 Conjunctions and disjunctions

Statements can be combined in various ways to give more complicated statements.

Inserting the word ‘and’ between two statements P and Q gives a new statement, called the **conjunction** of P and Q , which is true if both of P and Q are true, and false if at least one of P or Q is false.

For example, the variable proposition

x is greater than 0 and x is an integer

is true if *both* of the statements ' x is greater than 0' and ' x is an integer' are true, and false otherwise. Thus the combined statement is true if $x = 4$ but false if $x = 3.5$.

It is sometimes necessary to rephrase a statement to recognise that it is a conjunction. For example, a statement of the form ' P but not Q ' is in fact the conjunction ' P and not Q '. Thus, the statement

2 is prime but it is not odd

can be treated as the conjunction '2 is prime and 2 is not odd'.

Inserting the word 'or' between two statements P and Q also gives a new statement, the **disjunction** of P and Q , which is true if at least one of P or Q is true, and false if both of P and Q are false. Thus, the word 'or' is used in its inclusive sense in mathematical statements: ' P or Q ' means 'either P or Q or possibly both'.

For example, the variable proposition

x is greater than 0 or x is an integer

is true if *at least one* of the statements ' x is greater than 0' and ' x is an integer' is true, and false otherwise. Thus this combined statement is true if $x = 4$, $x = 3.5$ or $x = -4$ but false if $x = -3.5$.

Just as for conjunctions, it may be necessary to rephrase a statement to recognise that it is a disjunction. For example, statements of the form 'at least one of P or Q holds', or 'either P , or Q ', are different ways of expressing the disjunction ' P or Q '. So the statement

at least one of m or n is odd

can be treated as the disjunction

m is odd or n is odd.

Negating conjunctions and disjunctions

Since the statement ' P and Q ' is true exactly when both P and Q are true, its negation is true when at least one of P or Q is false. Thus the negation of ' P and Q ' is the statement 'not P or not Q '.

Worked Exercise A46

Negate the following conjunctions.

- (a) n is positive and p is prime
- (b) The sets A and B are both empty.
- (c) p is an odd prime.

Solution

- (a) This statement is false when at least one of ' n is positive' and ' p is prime' is false.

The negation is

n is less than or equal to 0, or p is not prime.

- (b) This statement can be expressed as

The set A is empty and the set B is empty.

The statement is false when at least one of 'the set A is empty' and 'the set B is empty' is false.

The negation is

The set A is non-empty or the set B is non-empty.

- (c) This statement can be expressed as

p is odd and p is a prime.

The statement is false when at least one of ' p is odd' and ' p is a prime' is false.

The negation is

p is even or p is not prime.

Similarly, the negation of ' P or Q ' is true exactly when both of P and Q are false; that is, exactly when 'not P and not Q ' is true. A little thought and some examples should convince you of this.

Worked Exercise A47

Negate the following disjunctions.

- (a) Either m or $m + 1$ is even
- (b) $x \geq 0$ or $y \geq 0$
- (c) Either $A = B$ or $A \cap B = \emptyset$.

Solution

- (a) This statement can be expressed as

m is even or $m + 1$ is even.

The statement is false when both ' m is even' and ' $m + 1$ is even' are false.

The negation is

m is odd and $m + 1$ is odd.

- (b) This statement is false when both ' $x \geq 0$ ' and ' $y \geq 0$ ' are false.

The negation is

$x < 0$ and $y < 0$.

- (c) This statement is false when both ' $A = B$ ' and ' $A \cap B = \emptyset$ ' are false.

The negation is

$A \neq B$ and $A \cap B \neq \emptyset$.

Exercise A103

Express concisely the negations of each of the following statements.

- (a) Both x and y are integers.
- (b) The integer m is even but the integer n is odd.
- (c) At least one of the integers m or n is odd.
- (d) Either $A = \emptyset$ or $B = \emptyset$.

1.3 Implications

Many mathematical statements are of the form 'if something, then something else', for example:

if $x > 2$, then $x^2 > 4$.

This type of statement is called an **implication**. An implication is made up of two statements, which in the example above are ' $x > 2$ ' and ' $x^2 > 4$ ', and can be expressed by combining these statements using the words 'if' and 'then'. In an implication 'if P , then Q ', the statement P is called the **hypothesis** of the implication, and the statement Q is called the **conclusion**.

It is important to be clear about exactly what an implication asserts. The statement above asserts only that if you know that $x > 2$, then you can be sure that $x^2 > 4$. It does not assert anything about the truth or falsity of ' $x^2 > 4$ ' when x is not greater than 2. In general, the implication

if P , then Q

asserts that if P is true, then Q is also true; that is, that it cannot happen that P is true and Q is false. The implication does not assert anything about the truth or falsity of Q when P is false.

If x is a real variable, then the statement

if $x > 2$, then $x^2 > 4$

is true because for every real number x for which ' $x > 2$ ' is true, ' $x^2 > 4$ ' is also true. Strictly speaking, this statement should be expressed as

for all $x \in \mathbb{R}$, if $x > 2$, then $x^2 > 4$.

However, it is conventional to omit the initial 'for all $x \in \mathbb{R}$ ', and interpret the statement as if it were there. We adopt this convention throughout this module (indeed, it is used in almost all mathematical texts), so statements of the form 'if P , then Q ', where P and/or Q are variable propositions, should be interpreted as applying to all possible values of the variables in the statements P and Q .

An implication does not have to be expressed using the words 'if' and 'then' – there are many other ways to convey the same meaning. The left-hand side of the table below lists some ways of expressing the implication 'if P , then Q '. The right-hand side gives examples for the particular implication 'if $x > 2$, then $x^2 > 4$ '.

Ways of writing 'if P , then Q '	Ways of writing 'if $x > 2$, then $x^2 > 4$ '
P implies Q	$x > 2$ implies $x^2 > 4$
$P \implies Q$	$x > 2 \implies x^2 > 4$
P is sufficient for Q	$x > 2$ is sufficient for $x^2 > 4$
P only if Q	$x > 2$ only if $x^2 > 4$
Q whenever P	$x^2 > 4$ whenever $x > 2$ (or: $x^2 > 4$, for all $x > 2$)
Q follows from P	$x^2 > 4$ follows from $x > 2$
Q is necessary for P	$x^2 > 4$ is necessary for $x > 2$
Q provided that P	$x^2 > 4$ provided that $x > 2$

The symbol \implies is read as 'implies', and it is commonly used in mathematical notation. The form ' P only if Q ' may seem strange at first; it asserts that the only circumstance in which P can be true is if Q is also true. In other words, if P is true, then Q must also be true – that is, P implies Q .

The notation \implies was first used by Nicolas Bourbaki in 1954. Nicolas Bourbaki was the pseudonym for a group of (mainly French) mathematicians who from 1935 over a period of thirty years produced an influential series of textbooks that were designed to present all of pure mathematics in a completely structured and axiomatic way. The name Bourbaki derives from that of a nineteenth-century French general, Charles Bourbaki, and was adopted by the group as a reference to a prank lecture by a student.



The founders of the Bourbaki group

The next exercise is for you to practise working with implications. In Section 2 you will see how to formally prove or disprove statements like those in parts (b) and (c). Whether the statement in part (a) is true or false can be established by algebraic manipulation.

Exercise A104

Rewrite each of the following statements in the form ‘if P , then Q ’. In each case, state whether you think the implication is true. You are not asked to justify your answers.

- (a) $x^2 - 2x + 1 = 0 \implies (x - 1)^2 = 0$.
- (b) Whenever n is odd, so is n^3 .
- (c) Every integer that is divisible by 3 is also divisible by 6.
- (d) $x > 2$ only if $x > 4$.
- (e) $x^3 \leq 0$ provided that $x \leq 0$.

Many theorems have statements of the form ‘Let P . Then Q ’. This is an alternative way to express a theorem of the form ‘if P , then Q ’. You have already met several theorems stated in this form – for example, the Division Theorem (Theorem A9 in Unit A2).

Theorem A9 Division Theorem

Let a and n be integers, with $n > 0$. Then there are unique integers q and r such that

$$a = qn + r, \quad \text{with } 0 \leq r < n.$$

The theorem could be restated as follows.

Theorem A9 Division Theorem (version 2)

If a and n are integers, with $n > 0$, then there are unique integers q and r such that

$$a = qn + r, \quad \text{with } 0 \leq r < n.$$

The negation of an implication

Contrary to what you might expect, the negation of an implication is *not* another implication – rather, it is a conjunction. To see why, it might help to think about the implication

if P , then Q

as asserting

it is not the case that P is true and Q is false.

Thus, *negating* the implication is equivalent to asserting that it *is* the case that P is true and Q is false, which is the conjunction

P and not Q .

A non-mathematical example might be helpful here. Consider the statement

If it snows before the next train to London is due to leave, then the next train to London gets cancelled.

If you want to negate this statement, you need to think about what has to happen in order for it to be false: that occurs if it snows before the next train to London is due to leave and the train leaves anyway. So the negation is

It snows before the next train to London is due to leave, and the next train to London does not get cancelled.

You will need to work with negations of implications when you meet *counterexamples* later in Section 2, so it will help to practise negating implications with mathematical content. This is the topic of the next worked exercise and exercise.

Here and later in the unit, we sometimes use brackets to avoid ambiguity when the conclusion of an implication is a conjunction or a disjunction. For example, in the implication

if the product mn is odd, then $(m \text{ is odd and } n \text{ is odd})$,

the conclusion is the conjunction ' m is odd and n is odd'. Enclosing this conclusion in brackets eliminates any possible confusion with the conjunction of the implication

if the product mn is odd, then m is odd

and the statement ' n is odd'.

Worked Exercise A48

Write down the negations of each of the following implications.

- (a) If m is odd, then m^2 is even.
- (b) If m divides 12, then (m divides 3 or m divides 4).

Solution

- (a) The statement ‘if m is odd, then m^2 is even’ can be restated as ‘it is not the case that m is odd and m^2 is not even’.

The negation is

m is odd and m^2 is not even,

that is,

m is odd and m^2 is odd.

- (b) The implication has the form ‘if m divides 12, then Q ’, where Q is the statement ‘ m divides 3 or m divides 4’. We can restate the implication in the form ‘it is not the case that (m divides 12 and not Q)’.

The negation of ‘ m divides 3 or m divides 4’ is

m does not divide 3 and m does not divide 4.

Therefore the negation of the implication is

m divides 12, and m divides neither 3 nor 4.

Exercise A105

Write down the negations of each of the following implications.

- (a) If m and n are odd, then $m + n$ is odd.
 - (b) If $A = \emptyset$, then ($A \cup B = \emptyset$ or $B - A = \emptyset$).
- (For part (b), remember that $B - A$ denotes the set of elements of B that are not elements of A .)

The converse of an implication

Given any implication, we can form another implication, called its **converse**. The converse of the implication ‘if P , then Q ’ is the implication

if Q , then P .

For example, the converse of the implication

if $x > 2$, then $x^2 > 4$

is

if $x^2 > 4$, then $x > 2$.

In this example, the original implication is true, and its converse is false (to see that the converse is false consider, for example, $x = -3$). It is also possible for an implication and its converse to be both true, or both false. In other words, knowledge of whether an implication is true or false tells you *nothing at all* about whether its converse is true or false. You should remember this important fact whenever you read or write implications.

To help you remember these facts about implications, you may again find it helpful to consider non-mathematical examples. For example, the implication

if Rosie is a sheep, then Rosie is less than two metres tall

is true, but its converse,

if Rosie is less than two metres tall, then Rosie is a sheep,

certainly is not true!

Exercise A106

For each of the following implications about integers m and n , write down its converse and state whether you think the implication, its converse or both are true. You are not asked to justify your answers.

- (a) If m and n are both odd, then $m + n$ is even.
- (b) If one of the pair m, n is even and the other is odd, then $m + n$ is odd.

The contrapositive of an implication

Given any implication, we can form a further implication, called its **contrapositive**. Unlike the converse, the contrapositive is *equivalent* to the original implication. The contrapositive of the implication ‘if P , then Q ’ is

if not Q , then not P .

For example, the contrapositive of the implication

if x is an integer, then x^2 is an integer

is the implication

if x^2 is not an integer, then x is not an integer.

You can think of an implication and its contrapositive as asserting the same thing, but in different ways. You should take a few moments to convince yourself of this in the case of the example just given.

Try this also with the following non-mathematical example. The contrapositive of the implication

if Rosie is a sheep, then Rosie is less than two metres tall

is

if Rosie is not less than two metres tall, then Rosie is not a sheep,

or, more simply,

if Rosie is at least two metres tall, then Rosie is not a sheep.

Contrapositive implications are a key ingredient of an important method of proof, proof by *contraposition*, that you will meet in Subsection 3.2. For now, it is important to remember the distinction between the converse of an implication, which is *not* equivalent to the implication, and its contrapositive, which is. A little practice should help you remember this distinction.

Exercise A107

For each of the following implications about integers m and n , write down its converse and its contrapositive and state whether you think the converse, the contrapositive or both are true. You are not asked to justify your answers.

- (a) If the product mn is even, then at least one of m or n is even.
- (b) If q divides the product mn , then (q divides m or q divides n).

1.4 Equivalences

The statement

if P , then Q , and if Q , then P ,

which asserts that the implication ‘if P , then Q ’ and its converse are *both* true, is usually expressed more concisely as

P if and only if Q .

Recall that ‘ P if Q ’ means ‘ $Q \implies P$ ’, and ‘ P only if Q ’ means ‘ $P \implies Q$ ’, so the phrase ‘if and only if’ is rather natural in this context.

If the statement ‘ P if and only if Q ’ is true, then P and Q are either both true or both false – in other words, if either one of P or Q is true, then so is the other.

Here are two examples:

- 1. n is odd if and only if n^2 is odd
- 2. $x > 2$ if and only if $x^2 > 4$.

Statements like these are called **equivalences**.

Equivalence 1 above is true because both the implications ‘if n is odd, then n^2 is odd’ and ‘if n^2 is odd, then n is odd’ are true. However, equivalence 2 is false because the implication ‘if $x^2 > 4$, then $x > 2$ ’ is false.

You have met equivalences before. For example, the Factor Theorem (Theorem A2 in Unit A2) contains an equivalence in its statement.

Theorem A2 Factor Theorem (in \mathbb{R})

Let $p(x)$ be a real polynomial, and let $\alpha \in \mathbb{R}$. Then $p(\alpha) = 0$ if and only if $x - \alpha$ is a factor of $p(x)$.

As with implications, there are many different ways to express equivalences. The table below lists some ways in which this can be done, with illustrations using example 1 above.

Ways of writing ‘ P if and only if Q ’	Ways of writing ‘ n is odd if and only if n^2 is odd’
$P \iff Q$	$n \text{ is odd } \iff n^2 \text{ is odd}$
P is equivalent to Q	$n \text{ is odd}$ is equivalent to $n^2 \text{ is odd}$
P is necessary and sufficient for Q	$n \text{ is odd}$ is necessary and sufficient for n^2 to be odd

The symbol \iff is commonly used to denote equivalences. It is usually read as ‘if and only if’, or sometimes as ‘is equivalent to’.

It is important to remember that the symbol \iff denotes equivalence between statements rather than equality between expressions, and should never be used in place of $=$. For example, it is *incorrect* to write $x^2 - 1 \iff (x + 1)(x - 1)$, but correct to write either

$$x^2 - 1 = (x + 1)(x - 1),$$

or

$$x^2 - 1 = 0 \iff (x + 1)(x - 1) = 0.$$

Exercise A108

For each of the following equivalences about integers, write down the two implications that it asserts, state whether you think each implication is true and hence state whether you think the equivalence is true. You are not asked to justify your answers.

- (a) The product mn is odd if and only if both m and n are odd.
- (b) The product mn is even if and only if both m and n are even.

In some cases, it is helpful to think of the equivalence $P \iff Q$ in terms of $P \implies Q$ and the implication ‘not $P \implies$ not Q ’. Recall that $Q \implies P$ is equivalent to its contrapositive ‘not $P \implies$ not Q ’. Therefore, since $P \iff Q$ asserts that both $P \implies Q$ and $Q \implies P$ hold, an alternative way to express the equivalence is to assert both

$$P \implies Q \text{ and } (\text{not } P \implies \text{not } Q).$$

For example, the equivalence

$$m \text{ is even} \iff m^2 \text{ is even}$$

can be expressed as

$$(m \text{ is even} \implies m^2 \text{ is even}) \text{ and } (m \text{ is odd} \implies m^2 \text{ is odd}).$$

Theorem A11 in Unit A2 contains an equivalence stated in this form.

Theorem A11

Let n and a be positive integers, with a in \mathbb{Z}_n .

- If a and n are coprime, then a has a multiplicative inverse in \mathbb{Z}_n .
- If a and n are not coprime, then a does not have a multiplicative inverse in \mathbb{Z}_n .

Thus, this theorem can be stated more succinctly as follows.

Theorem A11 (version 2)

Let n and a be positive integers, with a in \mathbb{Z}_n . Then a has a multiplicative inverse in \mathbb{Z}_n if and only if a and n are coprime.

We will prove this theorem in Subsection 3.1.

Although a mathematical statement should normally be interpreted as meaning precisely what it says – no more and no less – there is one common exception to this rule. When giving a *definition*, we usually write ‘if’ when we really mean ‘if and only if’. You have seen many examples of definitions in this form throughout Units A1 and A2 – below are two specific ones.

Definition

A set A is a subset of a set B if each element of A is also an element of B .

This definition (from Subsection 2.5 of Unit A1) is really stating that the two statements

A is a subset of B

and

each element of A is also an element of B

are *equivalent*. Below is the second example (from Subsection 3.2 of Unit A2).

Definition

Let n be a positive integer. Two integers a and b are **congruent modulo n** if $a - b$ is a multiple of n ; that is, if a and b have the same remainder on division by n .

Again, this definition is really saying that the statements ‘ a and b are congruent modulo n ’ and ‘ $a - b$ is a multiple of n ’ are equivalent.

1.5 Universal and existential statements

Many mathematical statements include the phrase ‘for all’, or another expression with the same meaning. Here are a few examples.

1. $x^2 \geq 0$ for all real numbers x .
2. Every multiple of 6 is divisible by 3.
3. $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ for each positive integer n .
4. Any rational number is a real number.

Statements of this type are known as **universal** statements, and the phrase ‘for all’, and its equivalents, are referred to as the **universal quantifier**.

The universal quantifier is sometimes denoted by the symbol \forall ; for example, the first universal statement above might be abbreviated as

$$\forall x \in \mathbb{R}, x^2 \geq 0,$$

which is read as ‘for all x in \mathbb{R} , x squared is greater than or equal to zero’.

Statements that begin with a phrase like ‘There are no ...’ or ‘There does not exist ...’ are universal statements because they can be rephrased in terms of ‘for all’. For example, the statement

there is no integer n such that $n^2 = 3$

can be rephrased as

for all integers n , $n^2 \neq 3$.

In Subsection 1.3 you met an important class of universal statements. Recall that implications of the form

$$P(x) \implies Q(x),$$

should strictly be expressed as ‘for all x , if $P(x)$, then $Q(x)$ ’, but the initial ‘for all x ’ is generally omitted by convention. So implications where the hypothesis and the conclusion are variable propositions are in fact universal statements where the universal quantifier is omitted. For example, the statement

if n is a multiple of 6, then n is a multiple of 3

means in fact

for all integers n , if n is a multiple of 6, then n is a multiple of 3.

We now turn to another type of statement with a quantifier. Some mathematical statements include the phrase ‘there exists’, or another expression with the same meaning. Here are a few examples.

1. *There exists* a real number that is not a rational number.
2. *There is* a real number x such that $\cos x = x$.
3. *Some* multiples of 3 are not divisible by 6.
4. The equation $x^3 + x^2 + 5 = 0$ has *at least one* real solution.

Statements of this type are known as **existential** statements, and the phrase ‘there exists’ and its equivalents are referred to as the **existential quantifier**.

In the third example, the word *some* is used to mean ‘at least one’, rather than several. It is important to remember that this is the standard mathematical usage of ‘some’.

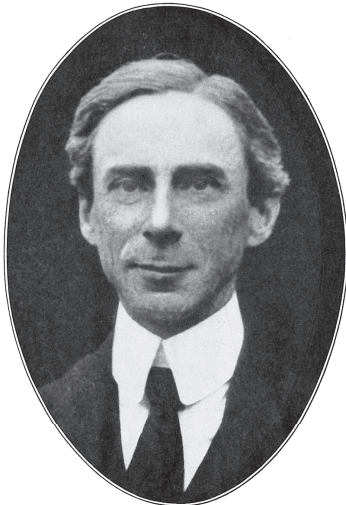
The existential quantifier is sometimes denoted by the symbol \exists ; for example, the second existential statement above might be abbreviated as

$$\exists x \in \mathbb{R} \text{ such that } \cos x = x,$$

which is read as ‘there exists x in \mathbb{R} such that $\cos x$ equals x ’.



Giuseppe Peano



Bertrand Russell



Gerhard Gentzen

The symbol \exists was introduced by Giuseppe Peano (1858–1932) in 1897 and was used by Bertrand Russell (1872–1970) and Alfred North Whitehead (1861–1947) in their monumental *Principia Mathematica* (1910–1913). In 1935 Gerhard Gentzen (1909–1945) introduced the \forall symbol. He called it the All-Zeichen (all character), in analogy with \exists which Gentzen said he borrowed from Russell.

In natural language, the word ‘any’ can mean either ‘every’ or ‘at least one’, as in ‘any fool could do that’ and ‘did you win any prizes?’. In mathematics, the meaning depends on the context in a similar way. We try to avoid using ‘any’ where it might cause confusion.

As already mentioned, it is often necessary to negate statements; for example, this is the case when we consider proof by contradiction or proof by contraposition, which you will meet in Section 3. The negation of universal and existential statements needs to be treated with particular care. The negation of a universal statement is an existential statement, and vice versa. This is illustrated by the examples in the table below.

Statement	Negation
Every integer is a real number.	There exists an integer that is not a real number.
There is an even prime number.	Every prime number is odd.
The equation $x^2 + 4 = 0$ has a real solution.	For all real numbers x , $x^2 + 4 \neq 0$.

Exercise A109

Express concisely the negations of each of these statements.

- (a) There is a real number x such that $\cos x = x$.
- (b) There exists an integer that is divisible by 3 but not by 6.
- (c) Every real number x satisfies the inequality $x^2 \geq 0$.

You have now met the negations of a number of different types of statements, and to conclude this section we collect them together in the table below.

Statement	Negation
P	not P
P and Q	not P or not Q
P or Q	not P and not Q
If P , then Q	P and not Q
For all x , P	There exists an x such that not P
There exists an x such that P	For all x , not P

2 Direct proof

The aim of this section and the next is to make you more familiar with the structures of various different types of mathematical proof. This section deals with *direct* methods of proof – that is, methods of proof which involve a series of logical steps leading from known facts and assumptions directly to the statement you wish to prove. In the next section you will consider *indirect* methods of proof.

Working through proofs, producing your own proofs and critically assessing mathematical arguments should help you to express your own mathematical thoughts and ideas more clearly.

In this module the proofs that you are asked to produce are simpler than many of the ones that are provided for you to read. Do not be discouraged if proof writing seems difficult at first: it is a skill that is acquired gradually. Working through the proofs that you meet is probably the most useful preparation. It is also important to study the more complex proofs that appear later in the module, and understand why they prove the statements that they claim to prove.

A *proof* of a mathematical statement is a logical argument that establishes that the statement is true. Here is a simple example.

Worked Exercise A49

Prove the following statement.

If n is an odd number between 0 and 10, then n^2 is also odd.

Solution

The odd numbers between 0 and 10 are 1, 3, 5, 7 and 9. The squares of these numbers are 1, 9, 25, 49 and 81, respectively, and these are all odd.

In the example above, there were only a small number of possibilities to consider, so it was easy to prove the statement by considering each one in turn. This method of proof is known as **proof by exhaustion** because we exhaust all possibilities. In contrast, it is not possible to prove the statement ‘If n is an odd number, then n^2 is also odd’ using proof by exhaustion because there are infinitely many possibilities to consider. Most mathematical statements that you will come across cannot be proved by exhaustion because there are too many possibilities to consider – usually infinitely many. Instead we must supply a general proof.

As an initial example of a general proof, we state and prove a result that applies to expressions of the form $a^n - b^n$. These expressions occur often in calculations, and you have probably already met the factorisations

$$\begin{aligned}a^2 - b^2 &= (a - b)(a + b), \\a^3 - b^3 &= (a - b)(a^2 + ab + b^2), \\a^4 - b^4 &= (a - b)(a^3 + a^2b + ab^2 + b^3),\end{aligned}$$

and so on. The following general result can be proved by multiplying out the expression on the right-hand side.

Theorem A12 Geometric Series Identity

Let $a, b \in \mathbb{R}$ and let n be a positive integer. Then

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}).$$

Proof Expanding the right-hand side of the equality gives

$$\begin{aligned}&(a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) \\&= a^n + a^{n-1}b + \cdots + a^2b^{n-2} + ab^{n-1} \\&\quad - (a^{n-1}b + a^{n-2}b^2 + \cdots + ab^{n-1} + b^n) \\&= a^n - b^n,\end{aligned}$$

as required. ■

The structure of the argument required in most proofs goes beyond the kind of algebraic verification used here. In the rest of this section, you will see how different techniques can be used for proofs that require arguments with a more complex structure.

2.1 Proving implications

Suppose we wish to prove that the implication $P \implies Q$ is true. We have to prove that whenever the statement P is true, the statement Q is also true. Often the best way to do this is to start out by *assuming* that P is true, and proceed as follows. If we know that the statement

$$P \implies P_1$$

is true for some statement P_1 , then we can deduce that P_1 is also true. Similarly, if we know that the statement

$$P_1 \implies P_2$$

is true for some statement P_2 , then we can deduce that P_2 is also true. In this way we can build up a sequence of statements

$$P, P_1, P_2, \dots,$$

each of which we know to be true under the assumption that P is true. The aim is to build up such a sequence



$$P, P_1, P_2, \dots, P_n, Q,$$

which leads to Q . If this can be achieved, then we have a proof of the implication $P \implies Q$. Here is an example.

Worked Exercise A50

Prove that if n is odd, then n^2 is odd.

Solution



 We have to prove that if n is odd, then n^2 is also odd. So we start by assuming that ‘ n is odd’ is true, and make use of the fact that n is odd if and only if it can be written in the form ‘2 times some integer plus 1’. 

Let n be an odd integer. Then

$$n = 2k + 1 \text{ for some integer } k.$$

Hence

$$n^2 = (2k + 1)^2 = (2k)^2 + 2(2k) + 1 = 2(2k^2 + 2k) + 1.$$

 We see that n^2 is odd because we have shown that n^2 is equal to 2 times some integer (that is, $2k^2 + 2k$) plus 1. 

Since $2k^2 + 2k$ is an integer, this shows that n^2 is an odd integer.

In the proof in Worked Exercise A50, statement P is ‘ n is odd’, and we start by assuming that this is true. Assumptions are generally introduced by words such as ‘let’, ‘suppose’ or ‘assume’. Statement P_1 is ‘ $n = 2k + 1$ for some integer k ’, and so on. We use words like ‘then’ and ‘hence’ to indicate that one statement follows from another. The string of equalities

$$n^2 = \dots = 2(2k^2 + 2k) + 1$$

in the proof can be regarded either as a sequence of three statements, namely

$$\begin{aligned} n^2 &= (2k + 1)^2, \\ n^2 &= (2k)^2 + 2(2k) + 1, \\ n^2 &= 2(2k^2 + 2k) + 1, \end{aligned}$$



or as a single statement asserting the equality of all four expressions.

Many of the true statements about odd and even integers that appeared in the exercises in the last subsection can be proved using ideas similar to those of the proof in Worked Exercise A50; that is, we write an odd integer as $2 \times \text{some integer} + 1$, and an even integer as $2 \times \text{some integer}$. (Similarly, we can often prove statements about multiples of 3 by writing each such number as $3 \times \text{some integer}$, and so on.) Here is another example.

Worked Exercise A51



Prove that the sum of two odd integers is even.

Solution

 We start by considering two odd integers, and then consider their sum. 

Let m and n be odd integers. Then

$$m = 2k + 1 \text{ and } n = 2l + 1 \text{ for some integers } k \text{ and } l.$$

 It is important to choose different symbols k and l here. We certainly cannot deduce from the first statement that $m = 2k + 1$ and $n = 2k + 1$ for some integer k ; that would be the case only if m and n were equal! 

Hence

$$m + n = (2k + 1) + (2l + 1) = 2k + 2l + 2 = 2(k + l + 1).$$

Since $k + l + 1$ is an integer, this shows that $m + n$ is an even integer.

We have seen that a sequence $P, P_1, P_2, \dots, P_n, Q$ of statements forms a proof of the implication $P \implies Q$ provided that each statement is shown to be true under the assumption that P is true. In Worked Exercises A50 and A51, each statement in the sequence was deduced from the statement

immediately before, but the sequence can also include statements that are deduced from one or more statements further back in the sequence, or statements that we know to be true from our previous mathematical knowledge. This is illustrated by Worked Exercise A52 below.

A fact that you may already know, which will be useful in Worked Exercise A52 and also later in this section, is that every integer greater than 1 has a unique expression as a product of prime numbers. For example, $6468 = 2 \times 2 \times 3 \times 7 \times 7 \times 11$, and this is the only way to express 6468 as a product of primes (except of course that we can change the order of the primes in the expression – the expression is unique *up to* the order of the primes). This fact is known as the *Fundamental Theorem of Arithmetic*.

Theorem A13 Fundamental Theorem of Arithmetic

Every integer greater than 1 can be written as a product of prime numbers. The factorisation is unique up to the order of the factors.

It is certainly not obvious that the Fundamental Theorem of Arithmetic is true! However, a proof is beyond the scope of this module.

Worked Exercise A52

Prove that for every integer n , the number $n^3 + 3n^2 + 2n$ is divisible by 6.

Solution

Let n be an integer. Now

$$n^3 + 3n^2 + 2n = n(n^2 + 3n + 2) = n(n+1)(n+2).$$

Thus $n^3 + 3n^2 + 2n$ is the product of three consecutive integers.

We know that out of any two consecutive integers, one must be divisible by 2, and out of any three consecutive integers, one must be divisible by 3.

It follows that the three factors n , $n+1$ and $n+2$ include at least one that is divisible by 2, and one that is divisible by 3. Thus both the primes 2 and 3 are factors of $n^3 + 3n^2 + 2n$.

Hence (by the Fundamental Theorem of Arithmetic) $n^3 + 3n^2 + 2n$ can be expressed as $2 \times 3 \times r$ for some integer r , and so it is divisible by $6 = 2 \times 3$.

The next exercise gives you practice in the techniques that you have seen so far in this subsection.

Exercise A110

Prove each of the following implications.

- (a) If n is an even integer, then n^2 is even.
- (b) If m and n are multiples of k , then so is $m + n$.
- (c) If one of the pair m, n is odd and the other is even, then $m + n$ is odd.
- (d) If n is a positive integer, then $n^2 + n$ is even.

If a proof of an implication is particularly simple, and each statement in the sequence follows directly from the one immediately before, then we sometimes present the proof by writing the sequence of statements in the form

$$P \implies P_1 \implies P_2 \implies P_3 \implies \cdots \implies P_n \implies Q.$$

This notation indicates that each of the statements $P \implies P_1$, $P_1 \implies P_2$, \dots , $P_n \implies Q$ is true. It is particularly appropriate for proofs that depend mostly on algebraic manipulation. Here is an example.

Worked Exercise A53

Prove that if $x(x - 2) = 3$, then $x = -1$ or $x = 3$.

Solution

$$\begin{aligned} x(x - 2) = 3 &\implies x^2 - 2x - 3 = 0 \\ &\implies (x + 1)(x - 3) = 0 \\ &\implies x + 1 = 0 \text{ or } x - 3 = 0 \\ &\implies x = -1 \text{ or } x = 3. \end{aligned}$$

It is worth noting that Worked Exercise A53 does not ask us to *solve* the equation, but, rather, to prove the implication

$$x(x - 2) = 3 \implies x = -1 \text{ or } x = 3.$$

By proving this implication, we showed that -1 and 3 are the only possibilities for solutions of the equation $x(x - 2) = 3$. We did not show that -1 and 3 actually *are* solutions, since for that it is necessary to prove also that if $x = -1$ or $x = 3$, then $x(x - 2) = 3$, that is, the *converse* of the given implication. Thus, strictly, we have not *solved* the equation!

Whenever we solve an equation, an implication and its converse must both be proved; in other words, we need to prove an equivalence. We will do this for the equation in Worked Exercise A53 in the next subsection (see Worked Exercise A55).

Even though proofs that depend on algebraic manipulation are among the easiest to produce, they still require care, as the following example shows.

Worked Exercise A54

Explain why the following proof that

$$4x^2 = x \implies x = \frac{1}{4}$$

is incorrect.

Claim (incorrect!)

If $4x^2 = x$, then $x = \frac{1}{4}$.

Proof (incorrect!)

$$\begin{aligned} 4x^2 = x &\implies 4x = 1 \\ &\implies x = \frac{1}{4}. \end{aligned}$$

**Solution**

The problem with this attempt lies in the implication

$$4x^2 = x \implies 4x = 1.$$

This implication is false: if $x = 0$, then the hypothesis $4 \times 0^2 = 0$ is true but the conclusion $4x = 1$ is false.

This happens because we can only divide both sides of the equation by the variable x if we suppose explicitly that $x \neq 0$, and then look separately at the case $x = 0$.

A correct deduction is as follows.

$$\begin{aligned} 4x^2 = x &\implies 4x^2 - x = 0 \\ &\implies x(4x - 1) = 0 \\ &\implies x = 0 \text{ or } x = \frac{1}{4}. \end{aligned}$$

Worked Exercise A54 requires a skill that is also helpful in writing proofs, namely the ability to evaluate arguments critically. The next two exercises give you further practice at spotting mistakes in deductions.

In the first of these exercises, and elsewhere later in the unit, you will meet an argument that involves rearranging an inequality. You should be familiar with the rules for rearranging inequalities from your previous mathematical studies, but if you need to refresh your memory, the rules are listed in the module Handbook. Inequalities are especially important in analysis, so you will study them more formally in the first of the analysis units, Unit D1 *Numbers*.

Exercise A111

Explain why the following deduction that $x = -1$ from the assumption $x \leq -1$ is incorrect.

Claim (incorrect!)

If $x \leq -1$, then $x = -1$.

Proof (incorrect!) We have that $x \leq -1 \implies (x+1)^2 \leq 0$, because

$$x \leq -1 \implies x+1 \leq 0 \implies (x+1)^2 \leq 0.$$

However, $(x+1)^2$ is the square of a real number, and a square can never be negative. Hence the only possibility is $x+1 = 0$, that is, $x = -1$.

Therefore, if $x \leq -1$, then $x = -1$. ■

In the next exercise you are asked to evaluate an incorrect argument that claims to prove a correct statement.

Exercise A112

Consider the following statement.

If $z_1 = 1 + 2i$ and $z_2 = \sqrt{3} - i\sqrt{2}$, then $|z_1| = |z_2|$.

Explain why the argument below is not a correct proof of this statement and write a correct proof.

Proof (incorrect!)

$$\begin{aligned} |z_1| = |z_2| &\implies |z_1|^2 = |z_2|^2 \\ &\implies 1^2 + 2^2 = (\sqrt{3})^2 + (-\sqrt{2})^2 \\ &\implies 1 + 4 = 3 + 2 \\ &\implies 5 = 5. \end{aligned}$$

Therefore $|z_1| = |z_2|$. ■

The incorrect proof in Exercise A112 shows a common proof pitfall: it is important to remember that assuming the statement P to be proved and using it to deduce a statement that is known to be true provides *no information at all* about the truth of P . Here is an archetypal example of this kind of incorrect argument.

Example (incorrect!)

$$\begin{aligned} 1 = -1 &\implies 1^2 = (-1)^2 \\ &\implies 1 = 1. \end{aligned}$$

In this example the conclusion $1 = 1$ is true, and each step in the deduction is valid, but the original statement, $1 = -1$, is most definitely false! As you learned in Subsection 1.3, an implication $P \implies Q$ does not give any information about the truth or falsity of Q when P is false.

2.2 Proving equivalences

We now discuss how to prove equivalences. Recall that the equivalence ‘ P if and only if Q ’ asserts that both the implication ‘ $P \implies Q$ ’ (‘ P only if Q ’) and its converse ‘ $Q \implies P$ ’ (‘ P if Q ’) are true. The best way to prove ‘ P if and only if Q ’ is usually to tackle each implication separately. However, if a simple proof of one of the implications can be found, in which each statement follows from the one before, then it is *sometimes* possible to ‘reverse all the arrows’ to obtain a proof of the converse implication. That is, if you have found a proof of the form

$$P \implies P_1 \implies P_2 \implies P_3 \implies \cdots \implies P_n \implies Q,$$

then you *may* find that also each of the following implications is true:

$$Q \implies P_n \implies \cdots \implies P_3 \implies P_2 \implies P_1 \implies P.$$

In this case you may be able to present the proofs of both implications at once, by writing

$$P \iff P_1 \iff P_2 \iff P_3 \iff \cdots \iff P_n \iff Q.$$

As with implications, this is particularly appropriate for proofs that depend mostly on algebraic manipulation. The next worked exercise gives a proof of this type showing that the implication in Worked Exercise A53 and its converse are both true. Remember that the symbol \iff is the one to use when solving equations or inequalities.

Worked Exercise A55

Prove that $x(x - 2) = 3$ if and only if $x = -1$ or $x = 3$.

Solution

$$\begin{aligned}
 x(x - 2) = 3 &\iff x^2 - 2x - 3 = 0 \\
 &\iff (x + 1)(x - 3) = 0 \\
 &\iff x + 1 = 0 \text{ or } x - 3 = 0 \\
 &\iff x = -1 \text{ or } x = 3.
 \end{aligned}$$

In Worked Exercise A55 we solved the equation $x(x - 2) = 3$: we showed that its solution set is $\{-1, 3\}$. The forward (\implies) part of the proof shows that if x satisfies $x(x - 2) = 3$, then $x = -1$ or $x = 3$; in other words, these are the only possible solutions of the equation. This is what we proved earlier in Worked Exercise A53. The backward (\impliedby) part shows that if $x = -1$ or $x = 3$, then x satisfies $x(x - 2) = 3$; in other words, these two values actually are solutions of the equation (note that if you were asked to prove only that $x = -1$ and $x = 3$ are solutions, and not that they are the *only* solutions, then it would be more natural to simply substitute each of these values in turn into the equation).

In the next worked exercise you are asked to prove a statement that involves sets. The proof requires a separate argument for each of the two implications that make up the equivalence.

Worked Exercise A56



Let A and B be any sets. Prove that

$$A \cup B = A \iff B \subseteq A.$$

Solution

 We prove the \implies direction first; that is, we assume that $A \cup B = A$. 

Suppose $A \cup B = A$.

 We want to deduce that $B \subseteq A$, that is, that if $x \in B$ then $x \in A$. So we pick an element $x \in B$. 

Let $x \in B$. Then x is also in the union $A \cup B$. But since $A \cup B = A$, this implies that $x \in A$. Therefore $B \subseteq A$, so we have shown that $A \cup B = A \implies B \subseteq A$.

 Now we prove the \impliedby direction. 

For the converse, assume that $B \subseteq A$.

☁ We want to show that $A \cup B = A$. The equality holds if both $A \cup B \subseteq A$ and $A \subseteq A \cup B$. The inclusion $A \subseteq A \cup B$ follows immediately from the definition of $A \cup B$. So we really want to show that the condition $A \cup B \subseteq A$ holds, that is, that if $x \in A \cup B$ then $x \in A$. ☁

Let $x \in A \cup B$. Then $x \in A$ or $x \in B$. If $x \in B$, then $x \in A$, because $B \subseteq A$ by assumption. Therefore $x \in A$, and so $A \cup B \subseteq A$.

Since $A \subseteq A \cup B$ always holds, it follows that $A \cup B = A$, so we have shown that $B \subseteq A \implies A \cup B = A$.

☁ Finally, we can state our conclusion. ☁

Hence $A \cup B = A \iff B \subseteq A$.

Exercise A113

Prove the following equivalences.

- (a) n is even $\iff n + 8$ is even
- (b) $A \subseteq A \cap B \iff A \subseteq B$.

Remember from Subsection 1.4 that an alternative way to express the equivalence $P \iff Q$ is to assert

$$P \implies Q \text{ and } (\text{not } P \implies \text{not } Q).$$

Thus the ‘if’ part of the equivalence – that is, $Q \implies P$ – can be proved by an argument that shows ‘not $P \implies$ not Q ’. This is sometimes convenient, as the next worked exercise shows.

Worked Exercise A57

Let n be a positive integer. Prove that

$$n \text{ is even} \iff n^3 \text{ is even.}$$

Solution

☁ We start by proving the \implies direction; that is, we assume that n is even and we want to deduce that n^3 is even. ☁



Let n be an even integer. Then

$$n = 2k \text{ for some integer } k.$$

Hence

$$n^3 = (2k)^3 = 2 \times 4k^3.$$

Since $4k^3$ is an integer, this shows that n^3 is an even integer. Thus we have shown that if n is even, then n^3 is even.

 We now need to prove the \Leftarrow direction; that is, we want to deduce that n is even from the assumption that n^3 is even. Writing $n^3 = 2k$ for some integer k does not seem to help in any obvious way to establish that n is even. Thus we try another approach: we assume that n is *not* even – that is, n is odd – and deduce that n^3 is odd. That is, we prove the contrapositive of the implication ‘if n^3 is even, then n is even’, which is equivalent to the implication. 

Now assume that n is odd. Then

$$n = 2k + 1 \text{ for some integer } k.$$

Hence

$$n^3 = (2k + 1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1.$$

Since $4k^3 + 6k^2 + 3k$ is an integer, this shows that n^3 is an odd integer.

Thus we have shown that if n is odd, then n^3 is odd, which is equivalent to the statement that n is even whenever n^3 is even.

Hence n is even $\iff n^3$ is even, as required.

In the solution to Worked Exercise A57, the proof of the \Leftarrow direction is an example of *proof by contraposition*, a method that you will look at in detail in Subsection 3.2.

If you decide to prove an equivalence by using a sequence of \iff , as in Worked Exercise A55, you must be sure that its use is valid at each step; in other words, that both implications hold. This advice holds in general for proofs where it may be tempting to use a sequence of equivalences, rather than to look at each implication separately. The next worked exercise shows an example of a rash use of a sequence of equivalences.

Worked Exercise A58

Consider the following exercise.

Let n be a positive integer. Prove that

$$n \text{ is a multiple of } 5 \text{ if and only if } n^2 \text{ is a multiple of } 5.$$

Explain why the proof below is incomplete.

Proof (incorrect!)

$$\begin{aligned}
n \text{ is a multiple of } 5 &\iff n = 5k \text{ for some integer } k \\
&\iff n^2 = 25k^2 \text{ for some integer } k \\
&\iff n^2 = 5(5k^2) \text{ for some integer } k \\
&\iff n^2 \text{ is a multiple of } 5.
\end{aligned}$$

**Solution**

The issue lies in the last equivalence in the sequence. While the implication

$$n^2 = 5(5k^2) \text{ for some integer } k \implies n^2 \text{ is a multiple of } 5$$

is clearly true, the converse implication

$$n^2 \text{ is a multiple of } 5 \implies n^2 = 5(5k^2) \text{ for some integer } k$$

requires further justification. The assumption ‘ n^2 is a multiple of 5’ tells us that $n^2 = 5l$ for some integer l , but does not immediately warrant the conclusion that n^2 can be written in the form $5(5k^2)$. There is a difference between stating that a given number is a multiple of 5 and stating that it is a multiple of 5 written in the specific form $5(5k^2)$ for some integer k .

In the solution to Worked Exercise A58, separating the two implications to be proved would have helped avoid the issue with the incorrect proof. In Worked Exercise A70 in Section 3.2 you will see a proof of the implication

if n^2 is a multiple of 5, then n is a multiple of 5

by *contraposition*, the method that we also used to prove the \iff direction in Worked Exercise A57. This implication can also be proved directly by using the Fundamental Theorem of Arithmetic and the fact that if a prime number p divides a product ab , then p divides a or p divides b .

Many theorems whose statement contains an equivalence have the form

If P , then (Q if and only if R).

or, equivalently,



Suppose P . Then (Q if and only if R).

In these cases, the assumption P holds throughout the proof. In addition, you assume Q when proving the implication ‘if Q , then R ’, and you assume R when you prove the converse implication ‘if R , then Q ’. The Factor Theorem (Theorem A2 in Unit A2) has this form, and you already know enough to work through its proof.

This proof is longer and it may require more work to understand than the examples you have seen so far. However, it is a good example of how the ideas in this subsection, and in previous ones, appear in mathematical practice. If you get stuck with the details of the deductions, try to concentrate on the structure of the proof and come back to it when you have had more practice.

Theorem A2 Factor Theorem (in \mathbb{R})

Let $p(x)$ be a real polynomial, and let $\alpha \in \mathbb{R}$. Then $p(\alpha) = 0$ if and only if $x - \alpha$ is a factor of $p(x)$.

Proof  Throughout the proof, we assume that $p(x)$ is a real polynomial and that $\alpha \in \mathbb{R}$. Under these assumptions, we need to prove an equivalence. We tackle each implication separately, and we start with the ‘if’ direction. So we start by assuming that $x - \alpha$ is a factor of $p(x)$. 

Assume first that $x - \alpha$ is a factor of $p(x)$, that is, assume that

$$p(x) = (x - \alpha)q(x)$$

for some real polynomial $q(x)$ whose degree is lower than the degree of $p(x)$. Then

$$p(\alpha) = (\alpha - \alpha)q(\alpha) = 0,$$

as required.

 We now prove the ‘only if’ direction, so we assume that $p(\alpha) = 0$. 

Now assume that $p(\alpha) = 0$, and let

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_n \neq 0$. Since $p(\alpha) = 0$, we have

$$\begin{aligned} p(x) &= p(x) - p(\alpha) \\ &= (a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) \\ &\quad - (a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0) \\ &= a_n (x^n - \alpha^n) + a_{n-1} (x^{n-1} - \alpha^{n-1}) + \cdots + a_1 (x - \alpha), \end{aligned}$$

since the constant terms a_0 cancel.

Now, by Theorem A12 (the Geometric Series Identity), we know that $x - \alpha$ is a factor of each of the bracketed terms in this last expression, and so it is a factor of $p(x)$, as required.

This concludes our proof. 

So far we have discussed proof only in the context of implications (and equivalences – though an equivalence is just two implications). Much of what we have said extends to proofs of other types of statements. A statement Q that is not an implication can be proved by building up a sequence of statements leading to Q in the way that we have seen for an

implication, except that there is no assumption P to be made at the start. Instead, the first statement in the sequence must be one that we know to be true from our previous mathematical knowledge.

In the next section we apply what you have learned so far to proving existential and universal statements.

2.3 Proving existential and universal statements

Statement 4 at the start of Subsection 1.1 is an example of a statement that is not an implication, nor an equivalence – it is an existential statement:


There is a real number x such that $\cos x = x$.

Existential statements can sometimes be proved by finding an object that satisfies the property in the statement.

Worked Exercise A59


Prove that there is a positive real number x such that $x < \sqrt{x}$.

Solution

 Since x is assumed to be positive, the condition $x < \sqrt{x}$ is equivalent to $x^2 < x$, that is, to $x^2 - x < 0$. (Remember that the rules for rearranging inequalities are given in the module Handbook if you need to refer to them.)

Now

$$x^2 - x < 0 \iff x(x - 1) < 0.$$

The product $x(x - 1)$ is less than 0 if and only if one of x and $x - 1$ is positive and the other is negative. Since x is assumed to be positive, any positive value of x such that $x < 1$ satisfies the inequality. So we can take, for example, $x = \frac{1}{9}$. 

Let $x = \frac{1}{9}$. Then $\sqrt{x} = \frac{1}{3}$, and $\frac{1}{9} < \frac{1}{3}$.

Here is another example for you to try.

Exercise A114

Prove that there is an integer n such that $3^n > 9^n$.

However, constructing a mathematical object with a given property can be considerably harder than this, and even impossible: for example, we have no way to find an exact solution to the equation

$$\cos x = x,$$

and so we need an alternative way to prove Statement 4. We can note that the graphs of the functions $f(x) = \cos x$ and $g(x) = x$ intersect at least once, so the equation does have a solution. However, for a rigorous proof we need the Intermediate Value Theorem which is proved later in the module. In cases where an example is hard to find, other methods of proof should be tried. On the other hand, when an existential statement *can* be proved by explicitly describing a mathematical object, it is important to remember that *one* example suffices: it is bad style to give multiple examples.

To prove a *universal* statement about an infinite set, however, you always need to give a general argument. You have already seen many examples of this in this unit, since many of the statements you have met so far are universal, though the universal quantifier is often implicit. For example, the statement in Worked Exercise A50,

if n is odd, then n^2 is odd,

could be rephrased as

for all integers n , if n is odd, then n^2 is odd,

whilst the statement in Worked Exercise A52 contains an explicit universal quantifier:

for every integer n , the number $n^3 + 3n^2 + 2n$ is divisible by 6.

The proof of a universal statement is an argument, of the kind you have seen in previous examples in this unit, that applies to all the objects covered by the quantifier. It is important to remember that checking that the statement holds in particular instances, however many, does not constitute a proof of a universal statement about an infinite set.

2.4 Counterexamples

Proving that a statement is true can be difficult. However, you may suspect that a statement is false, and it can often (but not always!) be easier to deal with this situation, especially when the statement is universal.

For example, recall that statements of the form

$$P(x) \implies Q(x)$$

are in fact universal statements where the universal quantifier ‘for all x ’ is omitted by convention. So the negation of $P(x) \implies Q(x)$ is

There is x such that $P(x)$ and not $Q(x)$.

Thus to prove that $P(x) \implies Q(x)$ is false, you just have to give *one* example of a case where the statement $P(x)$ is true but the statement $Q(x)$ is false. Such an example is called a **counterexample** to the implication. Here are two examples.

Worked Exercise A60

Show that each of the following implications about integers is false, by giving counterexamples.

- (a) If the product mn is a multiple of 4, then both m and n are multiples of 2.
- (b) If n is prime, then $2^n - 1$ is prime.

Solution

- (a) Taking $m = 4$ and $n = 1$ provides a counterexample because then $mn = 4$, which is a multiple of 4, but n is not a multiple of 2. Hence the implication is false.
- (b) The number 11 is a counterexample because 11 is prime but $2^{11} - 1 = 2047$, which is not prime since $2047 = 23 \times 89$. Hence the implication is false.

Remember that just *one* counterexample is sufficient. For example, you can show that the statement

$$\text{if } x^2 > 4, \text{ then } x > 2$$

is false by considering the value $x = -3$. There is no need to show that every number x less than -2 is a counterexample, even though this is the case.

There is no general method for finding counterexamples. For some statements, such as the statement in Worked Exercise A60(a), a little thought about the statement should suggest a suitable counterexample. For other statements, the quickest method may just be to try out different values for the variable (or variables) until you find a counterexample. For example, for the statement in Worked Exercise A60(b) we can repeatedly choose a prime number n , calculate $2^n - 1$ and check whether it is prime.

In order to carry out this procedure, we need a method for checking whether a given number m is prime. We could simply check whether m is divisible by each of the integers between 2 and $m - 1$ inclusive, but this involves a large amount of calculation even for fairly small integers m . We can significantly reduce the amount of calculation needed by using the following fact, which holds for any integer $m \geq 2$:

If m is not divisible by any of the primes less than or equal to \sqrt{m} , then m is a prime number.

You will be asked to prove this statement in Subsection 3.2. Here is an example of its use.

Worked Exercise A61

Show that 127 is a prime number.

Solution

We have $\sqrt{127} = 11.3$ to one decimal place, so the primes less than or equal to $\sqrt{127}$ are 2, 3, 5, 7 and 11. Dividing 127 by each of these in turn gives a non-integer answer in each case, so 127 is prime.

Exercise A115

Give a counterexample to disprove each of the following implications.

- (a) If $m + n$ is even, then both m and n are even.
- (b) If $x < 2$, then $(x^2 - 2)^2 < 4$.
- (c) If n is a positive integer, then $4^n + 1$ is prime.

As with implications, you may sometimes suspect that an equivalence is false. To prove that an equivalence $P \iff Q$ is false, you have to show that at least one of the implications $P \implies Q$ and $Q \implies P$ is false, which you can do by providing a counterexample; that is, you need a case where one of P or Q is true, and the other is false.

Exercise A116

Show that the equivalence

$$x^2 = 9 \iff x = 3$$

is false.

2.5 Proof by induction

Mathematical induction is a powerful method of proof that is particularly useful for proving statements involving integers, but also has wider applications.

The great French mathematician Henri Poincaré (1854–1912) described proof by mathematical induction as ‘mathematical reasoning par excellence’.

Consider, for example, Statement 3 in our list at the beginning of Subsection 1.1:

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2 \text{ for each positive integer } n.$$

Let us denote the variable proposition

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

by $P(n)$. It is easy to check that $P(n)$ is true for small values of n ; for example

$$\begin{aligned} 1 &= 1^2, \\ 1 + 3 &= 4 = 2^2, \\ 1 + 3 + 5 &= 9 = 3^2, \end{aligned}$$

so certainly $P(1)$, $P(2)$ and $P(3)$ are all true. But how can we prove that $P(n)$ is true for all positive integers n ?

The method of induction works like this. Suppose that we wish to prove that a statement $P(n)$, such as the one above, is true for all positive integers n . Now suppose that we have proved that the following two statements are true.

1. $P(1)$.
2. If $P(k)$ is true, then so is $P(k + 1)$, for $k = 1, 2, \dots$

Let us consider what we can deduce from this. Certainly $P(1)$ is true, because that is statement 1. Also $P(2)$ is true because, by statement 2, if $P(1)$ is true, then so is $P(2)$. Similarly, by statement 2, $P(3)$ is true since $P(2)$ is. Since this process goes on for ever, we can deduce that $P(n)$ is true for all positive integers n . We thus have the following method.

Principle of Mathematical Induction

To prove that a statement $P(n)$ is true for $n = 1, 2, \dots$:

1. show that $P(1)$ is true
2. show that the implication $P(k) \implies P(k + 1)$ is true for $k = 1, 2, \dots$

Mathematical induction is often compared to pushing over a line of dominoes – this is illustrated in Figure 2. Imagine a (possibly infinite!) line of dominoes set up in such a way that if any one domino falls then the next domino in line will fall too – this is analogous to step 2 above. Now imagine pushing over the first domino – this is analogous to step 1. The result is that *all* the dominoes fall!

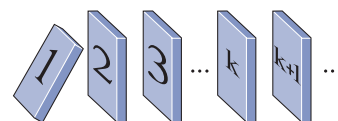
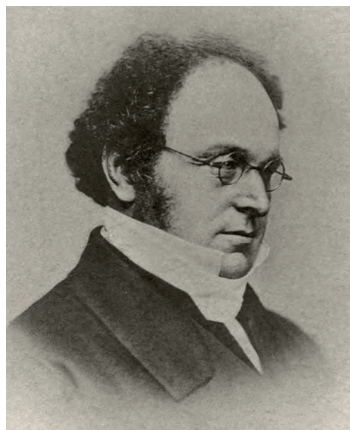


Figure 2 Toppling dominoes



Augustus De Morgan

Although indications of the method of mathematical induction can be found earlier, the first satisfactory formulations of the method are due to Pierre de Fermat (1601?–1665) in his work on number theory of 1630 (although not published until 1670) and Blaise Pascal (1623–1662) in a book on arithmetical triangles of 1654.

The term *mathematical induction* was introduced by the British mathematician Augustus De Morgan (1806–1871) in 1838 in an article he wrote for the *Penny Cyclopædia*.

In the next worked exercise we apply mathematical induction to prove the statement mentioned at the beginning of this subsection.

Worked Exercise A62

Prove that

$$1 + 3 + \cdots + (2n - 1) = n^2, \text{ for } n = 1, 2, \dots$$

Solution

Write out $P(n)$.

Let $P(n)$ be the statement $1 + 3 + \cdots + (2n - 1) = n^2$.

Next, carry out step 1, that is, check that $P(1)$ holds.

$P(1)$ is true because $1 = 1^2$.

Now proceed with step 2. State the assumption, $P(k)$.

Now let $k \geq 1$, and assume that $P(k)$ is true; that is,

$$1 + 3 + \cdots + (2k - 1) = k^2.$$

State the desired conclusion, $P(k + 1)$. The final term on the left-hand side of $P(k + 1)$ is $2(k + 1) - 1 = 2k + 1$.

We wish to deduce that $P(k + 1)$ is true; that is,

$$1 + 3 + \cdots + (2k - 1) + (2k + 1) = (k + 1)^2.$$

Now prove that $P(k) \implies P(k + 1)$. It should help to start with the left-hand side of the equality in $P(k + 1)$ and rearrange it in such a way that $P(k)$ can be used.

Now

$$\begin{aligned} 1 + 3 + \cdots + (2k - 1) + (2k + 1) &= (1 + 3 + \cdots + (2k - 1)) + (2k + 1) \\ &= k^2 + (2k + 1) \quad (\text{by } P(k)) \\ &= (k + 1)^2. \end{aligned}$$

This proves that $P(k) \implies P(k + 1)$, so we write out our conclusions.

Thus we have shown that

$$P(k) \implies P(k+1), \text{ for } k = 1, 2, \dots$$

Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \dots$

Exercise A117

Prove each of the following statements by mathematical induction.

- (a) $1 + 2 + \dots + n = \frac{1}{2}n(n+1)$, for $n = 1, 2, \dots$
 (b) $1^3 + 2^3 + \dots + n^3 = \frac{1}{4}n^2(n+1)^2$, for $n = 1, 2, \dots$

In the next worked exercise the argument used to prove $P(k+1)$ from $P(k)$ involves a more sophisticated algebraic manipulation than in Worked Exercise A62 and Exercise A117.

Worked Exercise A63

Prove that $2^{3n+1} + 5$ is a multiple of 7, for $n = 1, 2, \dots$

Solution

Let $P(n)$ be the statement

$$2^{3n+1} + 5 \text{ is a multiple of 7.}$$



$$P(1) \text{ is true because } 2^{3 \times 1 + 1} + 5 = 2^4 + 5 = 21 = 3 \times 7.$$

Now let $k \geq 1$, and assume that $P(k)$ is true; that is,

$$2^{3k+1} + 5 \text{ is a multiple of 7.}$$

We wish to deduce that $P(k+1)$ is true; that is,

$$2^{3(k+1)+1} + 5 = 2^{3k+4} + 5 \text{ is a multiple of 7.}$$

 We need an algebraic manipulation that creates the subexpression 2^{3k+1} on the right-hand side, so that we can use $P(k)$. Now, the exponent of 2 in $P(k+1)$ is $3k+4$. Note that $3k+4 = 3 + (3k+1)$, and $3k+1$ is the exponent of 2 in $P(k)$. 

Now

$$\begin{aligned} 2^{3k+4} + 5 &= 2^3 2^{3k+1} + 5 \\ &= 8 \times 2^{3k+1} + 5 \\ &= 7 \times 2^{3k+1} + 2^{3k+1} + 5. \end{aligned}$$

The first term here is a multiple of 7, and $2^{3k+1} + 5$ is a multiple of 7, by $P(k)$. Therefore $2^{3k+4} + 5$ is a multiple of 7. Thus we have shown that

$$P(k) \implies P(k+1), \text{ for } k = 1, 2, \dots$$

Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \dots$

Mathematical induction can be adapted to deal with situations that differ a little from the standard one. For example, if a statement $P(n)$ is not true for $n = 1$ but we wish to prove that it is true for $n = 2, 3, \dots$, then we can do this by following the usual method, except that in step 1 we prove that $P(2)$, rather than $P(1)$, is true. This is analogous to pushing over the second domino in the line: the result is that all the dominoes except the first fall!

Also, in step 2 we have to show that $P(k) \implies P(k+1)$ for $k = 2, 3, \dots$, rather than for $k = 1, 2, \dots$. In the next worked exercise we prove that a statement is true for $n = 7, 8, \dots$

Worked Exercise A64

Prove that $3^n < n!$ for all $n \geq 7$.

Solution

Let $P(n)$ be the statement ' $3^n < n!$ '.

 We are told to prove the statement for all $n \geq 7$, so we consider $P(7)$. 

$P(7)$ is true because $3^7 = 2187 < 5040 = 7!$.

Now let $k \geq 7$, and assume that $P(k)$ is true; that is,

$$3^k < k!.$$

We wish to deduce that $P(k+1)$ is true; that is,

$$3^{k+1} < (k+1)!.$$

Now

$$\begin{aligned} 3^{k+1} &= 3 \times 3^k \\ &< 3 \times k! \quad (\text{by } P(k)) \\ &< (k+1)k! \quad (\text{because } k \geq 7, \text{ and hence } k+1 \geq 8 > 3) \\ &= (k+1)!. \end{aligned}$$

 The conclusion $P(k) \implies P(k+1)$ holds for all $k \geq 7$. 

Hence $P(k) \implies P(k+1)$, for $k = 7, 8, \dots$

Hence, by mathematical induction, $P(n)$ is true, for $n = 7, 8, \dots$

$P(n)$ happens to be false for $n = 1, 2, \dots, 6$ in Worked Exercise A64 (you can check this if you like). However, the proof does not require any mention of this fact.

Exercise A118

Prove each of the following statements by mathematical induction.

- (a) $4^{2n-3} + 1$ is a multiple of 5, for $n = 2, 3, \dots$
- (b) $5^n < n!$ for all $n \geq 12$.



Proof by induction is also useful in many cases where the statement to be proved does not concern a property of the integers. You have already met at least one theorem that can be proved in this way: Theorem A3 in Unit A2 concerns all real polynomials that have as many distinct roots as their degree. The general statement can be proved by showing that it holds for all real polynomials of degree n with n distinct roots, for each $n \in \mathbb{N}$. Below you will see that the proof applies the Principle of Mathematical Induction to the degree n .

This proof, rather like the proof of the Factor Theorem in Subsection 2.2, is more advanced than the induction proofs you have seen so far in this subsection. Similar advice applies here as for the proof of the Factor Theorem: if the details of the deductions are not clear to you, try to concentrate on the structure of the proof, in particular on how the Principle of Mathematical Induction is used, and if necessary come back to the proof at a later stage.

Theorem A3

Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ be a real polynomial, and suppose that $p(x)$ has n distinct real roots $\alpha_1, \alpha_2, \dots, \alpha_n$. Then



$$p(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Proof  If we show that the result holds for all polynomials of degree n with n distinct roots, for $n \in \mathbb{N}$, then we have proved the general statement in the theorem. 

We argue by induction on the degree n . Let $P(n)$ be the statement

If $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ is a real polynomial with distinct roots $\alpha_1, \alpha_2, \dots, \alpha_n$, then

$$p(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

 Step 1 is to show that the statement holds for all polynomials of degree 1 with one real root; that is, we want to show that all polynomials of the form $a_1 x + x_0$ can be written in the form $a_1(x - \alpha_1)$, where α_1 is a root. 



$P(1)$ is true since if $p(x) = a_1x + a_0$ (where $a_1 \neq 0$) is a real polynomial with root α_1 , then $p(\alpha_1) = 0$. So

$$a_1\alpha_1 + a_0 = 0,$$

and so $a_0 = -a_1\alpha_1$. Thus

$$p(x) = a_1x - a_1\alpha_1 = a_1(x - \alpha_1),$$

as required.

 In order to carry out step 2, we assume that the theorem holds for all polynomials of degree k with k distinct real roots, and we want to deduce that it holds for all polynomials of degree $k + 1$. 

Suppose that $P(k)$ is true; that is, suppose that all polynomials of degree k with k distinct real roots have a factorisation of the form

$$a_k(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)$$

where $\alpha_1, \dots, \alpha_k$ are the roots.

We wish to deduce that $P(k + 1)$ holds; that is, all polynomials of degree $k + 1$ with $k + 1$ distinct real roots have a factorisation of the form

$$a_{k+1}(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{k+1})$$

where $\alpha_1, \dots, \alpha_{k+1}$ are the roots.



So let

$$q(x) = a_{k+1}x^{k+1} + a_kx^k + \cdots + a_1x + a_0,$$

where $a_{k+1} \neq 0$, be a polynomial of degree $k + 1$ with $k + 1$ distinct real roots. Let α_{k+1} be a root of $q(x)$. By the Factor Theorem, we have that $x - \alpha_{k+1}$ is a factor of $q(x)$, so

$$q(x) = (x - \alpha_{k+1})r(x),$$

where $r(x)$ is a polynomial of degree k . Moreover, the coefficient of x^k in $r(x)$ must be a_{k+1} .

 In order to apply $P(k)$ to $r(x)$, we also need to show that $r(x)$ has k distinct roots. 

Now let α be a root of $q(x)$ other than α_{k+1} . Then $q(\alpha) = 0$, that is,

$$(\alpha - \alpha_{k+1})r(\alpha) = 0.$$

Since $\alpha \neq \alpha_{k+1}$, we have $\alpha - \alpha_{k+1} \neq 0$, and so we must have $r(\alpha) = 0$. Thus α is a root of $r(x)$. Since $q(x)$ has $k + 1$ distinct real roots, including α_{k+1} , it follows that $r(x)$ has k distinct real roots.

 Since $r(x)$ is a polynomial of degree k with k distinct roots, we can apply $P(k)$. 

By $P(k)$, the polynomial $r(x)$ has a factorisation

$$r(x) = a_{k+1}(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k).$$

Thus

$$\begin{aligned} q(x) &= (x - \alpha_{k+1}) a_{k+1} (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k) \\ &= a_{k+1} (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)(x - \alpha_{k+1}). \end{aligned}$$

Therefore $q(x)$ has a factorisation of the required form. Thus we have shown that $P(k) \implies P(k+1)$, for $k = 1, 2, \dots$. Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \dots$ ■

The next exercise asks you to use induction to give a rigorous proof of the powers property of congruences that appears in Theorem A10 in Unit A2 (an informal proof was given in Unit A2). Recall that two integers a and b are congruent modulo n , written $a \equiv b \pmod{n}$, if $a - b$ is a multiple of n . In the proof, you will need to use the multiplication property of congruences, which was also part of Theorem A10:

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Exercise A119

Let a , b and n be integers. Use the Principle of Mathematical Induction and the multiplication property of congruences to prove that

if $a \equiv b \pmod{n}$, then $a^m \equiv b^m \pmod{n}$,

for $m = 1, 2, \dots$

Hint: Since you need to prove this statement for $m = 1, 2, \dots$, call the statement $P(m)$ and use induction on m .

Finally in this section, here is some advice to consolidate what you have learned about induction proofs. When you write a proof by induction make sure that you clearly identify the statement to be proved, $P(n)$, and structure your proof as follows:

- prove that $P(1)$ holds (or $P(n_0)$ for some initial $n_0 \neq 1$)
- write down $P(k)$ and assume that it holds for a general k
- state that we need to deduce $P(k+1)$, and write down $P(k+1)$
- deduce $P(k+1)$ from $P(k)$
- conclude that $P(n)$ holds for all natural numbers n (or for all $n \geq n_0$ where appropriate).

If you are unsure about your proof, review it and check that it follows this structure; in particular, check that $P(1)$ (or $P(n_0)$ where appropriate) is proved correctly, and that you have used $P(k)$ in the proof of $P(k+1)$.

Not all the proofs by induction that you will meet in the module materials, or in other textbooks, will match this format exactly, but this advice should help you *write* your own induction proofs. Below is an example of what can go wrong if you do not follow this template.

Worked Exercise A65

Consider the statement

$$2^1 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 2 \text{ for } n = 1, 2, \dots$$

Explain why the proof below is not a correct proof by induction, and write a correct proof.

Proof (incorrect!) Let $P(n)$ be the statement

$$2^1 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 2.$$

$P(1)$ is true because $2^1 = 2^{1+1} - 2 = 2^2 - 2$.

Now let $k \geq 1$. Assume $P(k)$; that is, assume that

$$2^1 + 2^2 + 2^3 + \cdots + 2^k = 2^{k+1} - 2.$$

We wish to deduce that $P(k+1)$ is true; that is

$$2^1 + 2^2 + 2^3 + \cdots + 2^{k+1} = 2^{k+2} - 2.$$

Dividing both sides of $P(k+1)$ by 2 gives

$$1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$$

hence

$$2 + 2^2 + \cdots + 2^k = 2^{k+1} - 2 \text{ by rearranging.}$$

Since we have obtained $P(k)$, which we assume is true, we know that $P(k+1)$ is true.

Therefore $P(n)$ is true for $n = 1, 2, \dots$ by mathematical induction. ■

Solution

Step 1 is correct, as is step 2 up to the statement of $P(k+1)$. However, step 2 is a deduction of $P(k)$ from $P(k+1)$, rather than the required proof that $P(k)$ implies $P(k+1)$. The fact that $P(k+1)$ implies a statement that we assume to be true does not constitute a proof of $P(k+1)$.

A correct version of step 2 is as follows.

Assume $P(k)$; that is, assume that

$$2^1 + 2^2 + 2^3 + \cdots + 2^k = 2^{k+1} - 2.$$

We wish to deduce that $P(k+1)$ is true; that is,

$$2^1 + 2^2 + 2^3 + \cdots + 2^{k+1} = 2^{k+2} - 2.$$

We have

$$\begin{aligned} 2^1 + 2^2 + \cdots + 2^k + 2^{k+1} &= (2^1 + 2^2 + 2^3 + \cdots + 2^k) + 2^{k+1} \\ &= 2^{k+1} - 2 + 2^{k+1} \quad (\text{by } P(k)) \\ &= 2 \times 2^{k+1} - 2 = 2^{k+2} - 2. \end{aligned}$$

Thus $P(k) \implies P(k+1)$, for $k = 1, 2, \dots$. Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \dots$.

Exercise A120

Consider the statement

$$2^n + 1 \leq 3^n, \quad \text{for } n = 1, 2, \dots$$

Explain why the following proof is not a correct induction argument, and give a correct proof.

Proof (incorrect!) Let $P(n)$ be the statement $2^n + 1 \leq 3^n$.

$P(1)$ is true since $2^1 + 1 = 3$.

Assume $P(k)$; that is, assume that $2^k + 1 \leq 3^k$.

We wish to deduce that $P(k+1)$ is true; that is

$$2^{k+1} + 1 \leq 3^{k+1}.$$

We have

$$\begin{aligned} 2^k + 1 &\leq 2(2^k + 1) \\ &= 2 \times 3^k \quad (\text{by } P(k)). \end{aligned}$$

Since $2 \times 3^k \leq 3 \times 3^k = 3^{k+1}$, we have that $P(k+1)$ holds.

Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \dots$ ■

3 Indirect proof

The proof methods that you will meet in this section are indirect in that they do not show directly that the statement to be proved is true. Instead, a proof by *contradiction* assumes that the statement to be proved is false and deduces a statement that cannot be true at the same time as some of the assumptions (or some other true mathematical statement), and in a proof by *contraposition* the contrapositive is proved, rather than the original implication.

3.1 Proof by contradiction

Sometimes a useful approach to proving a statement is to ask yourself, ‘Well, what if the statement were false?’. Consider the following example.

Worked Exercise A66

Prove that there is no positive real number a such that

$$a + \frac{1}{a} < 2.$$

Solution

Suppose that there *is* a positive real number a such that

$$a + \frac{1}{a} < 2.$$

Then, since a is positive, we have

$$a \left(a + \frac{1}{a} \right) < 2a,$$

which, on multiplying out and rearranging, gives

$$a^2 - 2a + 1 < 0;$$

that is,

$$(a - 1)^2 < 0.$$

But this is impossible, since the square of every real number is greater than or equal to zero. Hence we can conclude that there is no such real number a .

The proof above is an example of **proof by contradiction**. The idea is that if we wish to prove that a statement Q is true, then we begin by *assuming* that Q is *false*. We then attempt to deduce, using the method of a sequence of statements that you saw in Subsection 2.1, a statement that is definitely false, which in this context is called a **contradiction**. If this can be achieved, then since everything about our argument is valid except possibly the assumption that Q is false, and yet we have deduced a contradiction, we can conclude that the assumption is in fact false – in other words, Q is true.

You have already met this kind of proof: the proof of Theorem A1 given in Unit A2 is a proof by contradiction. It is repeated below, with further explanation of the thinking behind it.

Theorem A1

There is no rational number x such that $x^2 = 2$.

Proof 🧠 We assume that x is a rational number such that $x^2 = 2$ and aim for a contradiction. 🧠

Suppose for a contradiction that there is a rational number x such that $x^2 = 2$. Since x is rational, we can write $x = p/q$, where $p \in \mathbb{Z}$ and $q \in \mathbb{N}$. By replacing p/q by an equivalent fraction in lowest terms, if necessary, we may assume that the highest common factor of p and q is 1 (that is, that p and q are coprime). The equation $x^2 = 2$ now becomes

$$\frac{p^2}{q^2} = 2,$$

so

$$p^2 = 2q^2. \quad (1)$$

Therefore p^2 is even, which implies that p is even (we know that if p were odd, then p^2 would also be odd). So we can write $p = 2r$, where r is an integer, and equation (1) becomes

$$(2r)^2 = 2q^2.$$

Therefore we have

$$q^2 = 2r^2,$$

that is, q^2 is even. By a similar argument to that for p , we deduce that q is even.

🧠 If both p and q are even, then they are not coprime. 🧠

Since p and q are both even, 2 is a common factor of p and q . But we assumed p/q to be a fraction in its lowest terms, so this is a contradiction.

🧠 Since we have obtained a contradiction, our assumption that x is a rational number such that $x^2 = 2$ must be false. 🧠

Therefore no rational number x exists such that $x^2 = 2$. ■

Exercise A121

Show that there is no rational number x such that $x^3 = 2$.

The English mathematician G. H. Hardy (1877–1947) described proof by contradiction as ‘one of a mathematician’s finest weapons’. One of his favourite examples was a proof by contradiction of the existence of infinitely many primes. A version of the proof is given next. A proof of this result was originally given by Euclid in about 300 BCE, and it was essentially a proof by contradiction.



G. H. Hardy

Theorem A14


There are infinitely many prime numbers.

Proof Suppose that there are only finitely many primes, p_1, p_2, \dots, p_n . Consider the integer

$$N = p_1 p_2 p_3 \cdots p_n + 1.$$

This integer is greater than each of the primes p_1, p_2, \dots, p_n , so by our assumption it is not prime.

 We can use the Fundamental Theorem of Arithmetic (Theorem A13) to deduce that N has a prime factor. 

Now N has a prime factor, p say, by the Fundamental Theorem of Arithmetic. But p cannot be any of the primes p_1, p_2, \dots, p_n , since dividing any one of these into N leaves the remainder 1. Thus, p is a prime other than p_1, p_2, \dots, p_n . This is a contradiction, so our assumption that there are only finitely many primes must be false. It follows that there are infinitely many primes. 

In the next exercise you can practise proof by contradiction for statements that are similar to that in Worked Exercise A66, in that they assert the non-existence of numbers with a certain property.

Exercise A122

Use proof by contradiction to prove each of the following statements.

- (a) There are no real numbers a and b with $ab > \frac{1}{2}(a^2 + b^2)$.
- (b) There are no integers m and n with $5m + 15n = 357$.

The next worked exercise uses proof by contradiction to prove a general statement about sets.

Worked Exercise A67

Prove that, for any two sets A and B ,

$$A \cap (B - A) = \emptyset.$$

Solution

Suppose for a contradiction that $A \cap (B - A) \neq \emptyset$. Then there is an element, x , such that $x \in A \cap (B - A)$; that is, there is an x such that $x \in A$ and $x \in B - A$. But then, since $x \in B - A$, we have that $x \notin A$, which is a contradiction.

Therefore $A \cap (B - A) = \emptyset$, as required.



Proof by contradiction can sometimes be used to prove an implication. To prove an implication $P \implies Q$ by contradiction, you should begin by assuming that the implication is false, hoping for a contradiction. That is, you should assume that P is true and Q is false. If under these assumptions you can deduce a contradiction, then you can conclude that if P is true, then Q must also be true, which is the required implication. Here is an example.

Worked Exercise A68

Prove that if $n = ab$ where $n > 0$, then at least one of a and b is less than or equal to \sqrt{n} .

Solution

Suppose that $n = ab$ where $n > 0$.

 We start by assuming that the implication is false, which means that both a and b are greater than \sqrt{n} . We then try to deduce a contradiction. 

Suppose also that $a > \sqrt{n}$ and $b > \sqrt{n}$. Then

$$n = ab > (\sqrt{n})(\sqrt{n}) = n;$$

that is, $n > n$. This contradiction shows that the supposition that $a > \sqrt{n}$ and $b > \sqrt{n}$ must be false; that is, at least one of a and b is less than or equal to \sqrt{n} .

Exercise A123

Use proof by contradiction to prove that if $n = a + 2b$, where a and b are positive real numbers, then $a \geq \frac{1}{2}n$ or $b \geq \frac{1}{4}n$.

As a final example that applies what you have learned in this subsection to a result that you have already met, we give below a formal proof of Theorem A11 from Unit A2, restated as an equivalence. One of the implications is proved by contradiction.

The usual advice applies that if the details of the proof are not all clear, for now you should concentrate on the structure of the proof, in particular on how the ‘only if’ direction is proved by contradiction.

Theorem A11

Let n and a be positive integers, with a in \mathbb{Z}_n . Then a has a multiplicative inverse in \mathbb{Z}_n if and only if a and n are coprime.

Proof We assume that n is a positive integer and $a \in \mathbb{Z}_n$. We start by proving the ‘only if’ direction. We assume that a has a multiplicative inverse in \mathbb{Z}_n and we want to deduce that a and n are coprime. We argue by contradiction.

Suppose that a has a multiplicative inverse in \mathbb{Z}_n , and assume for a contradiction that a and n are not coprime, that is, that a and n have a common factor $d > 1$.

Let b be the multiplicative inverse of a in \mathbb{Z}_n ; then $b \times_n a = 1$, and so

$$ba = kn + 1$$

for some integer k , and therefore $ba - kn = 1$.

Any common factor of a and n is also a common factor of ba and kn , and therefore of $ba - kn$.

Since d is a common factor of a and n , we have that d divides $ba - kn$. But this is a contradiction, since $ba - kn = 1$ and $d > 1$.

The assumption that a and b are not coprime leads to a contradiction, so we conclude that a and b are coprime.

Therefore a and b are coprime.

We now prove the ‘if’ direction in the equivalence, so we start by assuming that a and n are coprime.

Now let a and n be coprime.

For this direction of the proof we use Euclid’s Algorithm, a method for finding the highest common factor of two positive integers that you met in Unit A2. By the Division Theorem, quoted in Subsection 1.3, we know that there are unique integers q_1 and r_1 such that

$$n = q_1a + r_1, \quad \text{with } 0 \leq r_1 < a.$$

Euclid’s Algorithm proceeds by applying the Division Theorem again to the remainder r_1 , and then successively repeating this step.

We apply Euclid’s Algorithm. From one step of the algorithm to the next, the remainder decreases by at least 1, so it must eventually reach 0. We have

$$\begin{array}{ll} n = q_1a + r_1 & 0 < r_1 < a \\ a = q_2r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 = q_3r_2 + r_3 & 0 < r_3 < r_2 \\ \vdots & \vdots \\ r_{m-2} = q_mr_{m-1} + r_m & 0 < r_m < r_{m-1} \\ r_{m-1} = q_{m+1}r_m + 0. & \end{array}$$

The final equation shows that r_m is a factor of r_{m-1} .

Since r_m is a factor of r_{m-1} , it is also a factor of $q_m r_{m-1}$, and therefore of $q_m r_{m-1} + r_m$. Hence r_m is also a factor of r_{m-2} , and so on up the list.

Therefore the penultimate equation shows that r_m is a factor of r_{m-2} , and so on. In this way, we find that r_m is a factor of all the remainders r_m, r_{m-1}, \dots, r_1 , and so of both a and n .

Since a and n are coprime by assumption, their only common factor is 1.

Since we assumed that a and n are coprime, we deduce that $r_m = 1$.

Therefore the penultimate equation gives

$$1 = r_{m-2} - q_m r_{m-1}.$$

By backwards substitution we find that there are integers k and d such that $1 = kn + da$. Hence $da = -kn + 1$, that is, $d \times_n a = 1$.

If $d \in \mathbb{Z}_n$, then d is a multiplicative inverse of a in \mathbb{Z}_n .

If $d \notin \mathbb{Z}_n$, we have $d \equiv b \pmod{n}$ for some $b \in \mathbb{Z}_n$, where $b \neq 0$ and $b \times_n a = 1$. Hence b is a multiplicative inverse of a in \mathbb{Z}_n .

Therefore in either case a has a multiplicative inverse in \mathbb{Z}_n , as required. ■

3.2 Proof by contraposition

Recall that the contrapositive of the implication ‘if P , then Q ’ is ‘if not Q , then not P ’, where ‘not P ’ and ‘not Q ’ denote the negations of the statements P and Q , respectively.

Since an implication and its contrapositive are equivalent, if you have proved one, then you have proved the other. Sometimes the easiest way to prove an implication is to prove its contrapositive instead. This is called **proof by contraposition**. Here is an example. The proof makes use of the following identity, which is a special case of the Geometric Series Identity (Theorem A12) that you met at the beginning of Section 2: for any real number x and any positive integer n , we have

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + x + 1). \quad (2)$$

Worked Exercise A69

Prove the following implication about positive integers n :



if $2^n - 1$ is prime, then n is prime.

Solution

We prove the contrapositive of the implication, which is

if n is not prime, then $2^n - 1$ is not prime.

Suppose that n is a positive integer that is not prime.

 We consider two cases separately: the cases $n = 1$ and $n > 1$. Splitting into separate cases is sometimes an effective way to proceed in a proof. 

If $n = 1$, then $2^n - 1 = 2 - 1 = 1$, which is not prime.

If $n > 1$, then since n is not prime by our assumption, we can write $n = ab$, where $1 < a, b < n$. Hence

$$\begin{aligned} 2^n - 1 &= 2^{ab} - 1 \\ &= (2^a)^b - 1 \\ &= (2^a - 1)((2^a)^{b-1} + \cdots + 2^a + 1), \end{aligned}$$

where the last line follows from equation (2) by taking $x = 2^a$ and $n = b$.

Now $2^a - 1 > 1$ since $a > 1$, and also $(2^a)^{b-1} + \cdots + 2^a + 1 > 1$ since both a and b are greater than 1. Hence $2^n - 1$ is not prime. We have thus proved the required contrapositive implication in both the cases $n = 1$ and $n > 1$. Hence the original implication is also true.

When proving results about integers, proof by contraposition is especially useful when the conclusion has the form ‘ n is even’, or ‘ n is odd’, or a combination of statements of this kind. Below is a different example that in fact gives a proof by contraposition of the missing implication in Worked Exercise A58 in Subsection 2.2.



Recall from Subsection 3.2 of Unit A2 that for integers a, b and n , $a \equiv b \pmod{n}$ if (and only if) a and b have the same remainder on division by n .

Worked Exercise A70

Prove the ‘if’ direction of the statement in Worked Exercise A58; that is, prove that, if n is a positive integer,

if n^2 is a multiple of 5, then n is a multiple of 5.

Solution

 We have seen in Worked Exercise A58 that the assumption ‘ n^2 is a multiple of 5’ does not help us reach the conclusion in any obvious way, so we try proving the contrapositive. 

We prove the contrapositive implication, which is

if n is not a multiple of 5, then n^2 is not a multiple of 5.

Suppose that n is not a multiple of 5.



Then, by the Division Theorem, n can be written as one of

$$5k + 1 \text{ or } 5k + 2 \text{ or } 5k + 3 \text{ or } 5k + 4,$$



for some integer k , and so one of the following holds:

$$n \equiv 1 \pmod{5} \text{ or } n \equiv 2 \pmod{5} \text{ or } n \equiv 3 \pmod{5} \text{ or } n \equiv 4 \pmod{5}.$$

We consider each of these cases.

 We use the powers property of congruences which you proved in Exercise A119. For congruences modulo 5 it follows from this result that if $a \equiv b \pmod{5}$, then $a^2 \equiv b^2 \pmod{5}$. 

If $n \equiv 1 \pmod{5}$, then $n^2 \equiv 1 \pmod{5}$. If $n \equiv 2 \pmod{5}$, then $n^2 \equiv 2^2 \equiv 4 \pmod{5}$. Similarly, if $n \equiv 3 \pmod{5}$, then $n^2 \equiv 9 \equiv 4 \pmod{5}$, and if $n \equiv 4 \pmod{5}$, then $n^2 \equiv 16 \equiv 1 \pmod{5}$.

 These cases cover all the possibilities for n^2 , and in each case the remainder on dividing n^2 by 5 is not zero. 

Therefore n^2 is not a multiple of 5, as required.

Since the contrapositive is true, the original implication is also true.

Exercise A124

Use proof by contraposition to prove each of the following statements about integers m and n .

- (a) If $n^3 + 2n + 1$ is even, then n is odd.
- (b) If mn is odd, then both m and n are odd.
- (c) If an integer $n > 1$ is not divisible by any of the primes less than or equal to \sqrt{n} , then n is a prime number.

Hint: Use the result of Worked Exercise A68.



The next worked exercise involves a statement about sets that can be proved rather neatly by contraposition.

Worked Exercise A71

Prove that, for any sets A and B ,

if $(A - B) \cup (B - A) = A \cup B$, then $A \cap B = \emptyset$.

Solution

 The hypothesis of the implication that we are required to prove is a more complex statement than the conclusion. It might be easier to prove the contrapositive since the negation of the conclusion, ' $A \cap B \neq \emptyset$ ', is a clearer hypothesis that is easier to understand. 

We prove the contrapositive implication, which is

if $A \cap B \neq \emptyset$, then $(A - B) \cup (B - A) \neq A \cup B$.

Suppose that $A \cap B \neq \emptyset$. Then there is an element x such that $x \in A$ and $x \in B$, so $x \in A \cup B$.

However, $x \notin A - B$, because $x \in B$. Similarly, $x \notin B - A$. Therefore $x \notin (A - B) \cup (B - A)$. So x is an element of $A \cup B$ that is not in $(A - B) \cup (B - A)$. Hence

$$(A - B) \cup (B - A) \neq A \cup B,$$

as required.

The contrapositive is true, therefore the original statement is also true.

Exercise A125

Let A and B be sets. Prove that

if $A \subseteq B$, then $A - B = \emptyset$.

The final exercise in this subsection asks you to read critically an attempted proof by contraposition.

Exercise A126

Consider the statement

if $n^3 + 3$ is even, then n is odd.

Explain why the argument below is not a correct proof of this statement, and give a correct proof.

Proof (incorrect!) We prove the contrapositive, that is

if n is odd, then $n^3 + 3$ is even.

Assume n is odd. Then $n = 2k + 1$ for some integer k , and so

$$\begin{aligned} n^3 + 3 &= (2k + 1)^3 + 3 \\ &= 8k^3 + 12k^2 + 6k + 1 + 3 \\ &= 8k^3 + 12k^2 + 6k + 4 \\ &= 2(4k^3 + 6k^2 + 3k + 2). \end{aligned}$$

This shows that $n^3 + 3$ is even, as required. ■

The exercise above is an example of a common pitfall when trying to prove a statement by contraposition, that is, a mistake in finding the contrapositive.

You may have found some of the ideas so far in this unit difficult to get used to; this is to be expected since reading and understanding mathematics, and writing mathematics clearly and accurately, can both be difficult at first. Your skills will improve as you gain experience. To accelerate this improvement, you should, when reading mathematics, try to make sure that you gain a clear understanding of exactly what each statement asserts. When writing mathematics, you should try to be as clear and accurate as you can. Include enough detail to make the argument clear, but omit any statements that are not necessary to reach the required conclusion. A good check is to read over your work and ask yourself whether you would be able to follow what you have written in six months' time, when you have forgotten the thoughts and rough work that led to it. Use the solutions to the exercises and worked exercises in the module as models for good mathematical writing.

You may find it helpful to revisit parts of Sections 1, 2 and 3 later in your study of the module.

4 Equivalence relations

In this section you can apply many of the ideas about careful, logical thinking and proof that you have learned in the previous sections of this unit to a new topic in which this approach is needed. This topic is the important one of *equivalence relations*. Equivalence relations occur throughout mathematics, and are particularly important in the group theory units of this module.

4.1 What is an equivalence relation?

As you would expect, an *equivalence relation* is a special type of relation, so we will start by looking at what is meant by a *relation*.

In everyday life we often work with *relations* between objects. For example, *is a child of* is a relation between people: we might say ‘Emma Smith *is a child of* Stephen Smith’, for instance. Other examples of relations between people include *is a descendant of* and *lives in the same street as*. An example of a relation between other types of object is *shares a border with*, between countries of the world. For instance, we might say ‘France *shares a border with* Germany’.

In mathematics, too, we often work with relations between objects. For example, *is a multiple of* is a relation between the numbers in the set \mathbb{N} . Thus we can make statements such as ‘6 *is a multiple of* 3’, which is true, and ‘5 *is a multiple of* 2’, which is false. Another example of a mathematical relation is *is parallel to*, applied to the lines in the plane.

It is sometimes useful to denote a mathematical relation by a symbol, and in this module we usually use the symbol \sim . For example, if we use \sim to denote the relation *is a multiple of*, then we write the statement ‘6 *is a multiple of* 3’ as $6 \sim 3$. The symbol \sim is known as *tilde* (pronounced ‘tilder’), and in mathematics is usually read as ‘twiddles’. So you can read the statement $6 \sim 3$ as ‘6 twiddles 3’. Alternatively, you can read it as ‘6 is related to 3’. (In some texts you may see the symbol R rather than \sim used for ‘is related to’, so $6 \sim 3$ would be written as $6 R 3$.)

Some frequently used relations have their own special symbols. For example, the relation *is less than* is usually denoted by the special symbol $<$. Examples of the use of this symbol are the statement $-2 < 1$, which is true, and the statements $1 < -2$ and $3 < 3$, which are both false.

Here is a precise definition of what we mean by a relation.

Definition

We say that \sim is a **relation** on a set X if, whenever $x, y \in X$, the statement $x \sim y$ is either true or false.

If \sim is a relation on a set X and $x \sim y$ is false for a particular pair of elements x and y in X , then we write $x \not\sim y$.

Here are some more examples of relations.

1. *Is equal to* is a relation on the set \mathbb{R} . This is because, for any x, y in \mathbb{R} , the statement ‘ x is equal to y ’ is either definitely true or definitely false. This relation is usually denoted by the special symbol $=$. For instance, the statement $3 = 3$ is true, and the statement $3 = 7$ is false. The relation ‘ $=$ ’ has the unusual property that for any real number x , the only real number y such that $x = y$ is x itself.

2. Is the derivative of is a relation on any set of functions. We can define

$$g \sim f \quad \text{if } g \text{ is the derivative of } f.$$

For example, let f , g and h be the real functions given by $f(x) = x^3$, $g(x) = 3x^2$ and $h(x) = 2e^x$. Then $g \sim f$ because g is the derivative of f , and $h \sim h$ because h is the derivative of h , but $f \not\sim g$ because f is not the derivative of g .

3. On \mathbb{C} , we can define a relation

$$z_1 \sim z_2 \quad \text{if } |z_1 - z_2| \leq 4;$$

that is, $z_1 \sim z_2$ if the distance between z_1 and z_2 in the complex plane is less than or equal to 4. For example, $(1 + i) \sim (2 - i)$ because

$$|(1 + i) - (2 - i)| = |-1 + 2i| = \sqrt{5} \leq 4,$$

but $(1 + i) \not\sim (3 + 5i)$ because

$$|(1 + i) - (3 + 5i)| = |-2 - 4i| = \sqrt{20} = 2\sqrt{5} > 4$$

(see Figure 3).

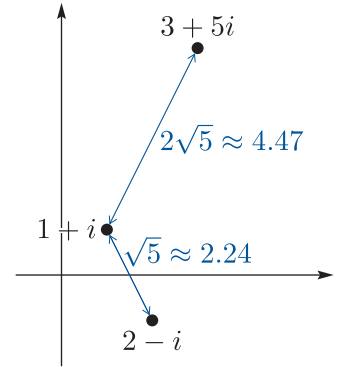


Figure 3 Some distances in the complex plane

Exercise A127

Let \sim be the relation on \mathbb{N} defined by

$$x \sim y \quad \text{if } x \text{ is a divisor of } y.$$

Which of the following statements are true?

- (a) $3 \sim 6$ (b) $6 \sim 3$ (c) $6 \sim 18$ (d) $6 \sim 6$

Exercise A128

Let \sim be the relation on \mathbb{R} defined by

$$x \sim y \quad \text{if } x - y \text{ is an integer.}$$

- (a) Which of the following statements are true?
 (i) $1.3 \sim 5.3$ (ii) $2.8 \sim 2.1$ (iii) $2.4 \sim -5.4$
- (b) (i) Write down a real number y such that $0.8 \sim y$.
 (ii) Write down a real number z such that $0.8 \not\sim z$.

In this section we are mainly interested in relations of a type known as *equivalence relations*. These are relations that have three special properties, as defined below.

Definition

A relation \sim on a set X is an **equivalence relation** if it has the following three properties.

E1 Reflexivity For all x in X ,

$$x \sim x.$$

E2 Symmetry For all x, y in X ,

$$\text{if } x \sim y, \text{ then } y \sim x.$$

E3 Transitivity For all x, y, z in X ,

$$\text{if } x \sim y \text{ and } y \sim z, \text{ then } x \sim z.$$

If a relation has the first, second or third property above, then we say that it is **reflexive**, **symmetric** or **transitive**, respectively.

The three properties reflexivity, symmetry and transitivity are independent in the sense that relations exist with every combination of the three properties.

Note that if a relation \sim is symmetric, then $x \sim y$ and $y \sim x$ mean the same, and we can write either of these interchangeably. For example, the relation $=$ on \mathbb{R} is symmetric, so $x = y$ and $y = x$ mean the same. The relation $<$ on \mathbb{R} is not symmetric, so $x < y$ and $y < x$ mean different things.

To help you understand the three properties, it can be helpful to think through whether they hold for some non-mathematical relations, as in the next worked exercise.

Worked Exercise A72

For each of the following non-mathematical relations on a set of people, state whether the relation is reflexive, symmetric and transitive, briefly justifying your answers, and hence state whether the relation is an equivalence relation.

- (a) ‘lives on the same street as’
- (b) ‘is a descendant of’

Solution

- (a) **E1** The relation ‘lives on the same street as’ is reflexive, because each person lives on the same street as themselves.
- E2** It is also symmetric, because if person A lives on the same street as person B, then it follows that person B lives on the same street as person A.
- E3** Finally, it is transitive, because if person A lives on the same street as person B, and person B lives on the same street as person C, then person A lives on the same street as person C.

Hence this relation is an equivalence relation.

- (b) **E1** The relation ‘is a descendant of’ is not reflexive, because a person is not a descendant of themselves.
- E2** Nor is it symmetric, because if person A is a descendant of person B, then it does not follow that person B is a descendant of person A.
- E3** However, it is transitive, because if person A is a descendant of person B, and person B is a descendant of person C, then it follows that person A is a descendant of person C.

Since this relation is not reflexive (or symmetric), it is not an equivalence relation.

Exercise A129

For each of the following non-mathematical relations on a set of people, state whether the relation is reflexive, symmetric and transitive, briefly justifying your answers, and hence state whether the relation is an equivalence relation.

- (a) ‘has sat next to’
- (b) ‘was born in the same year as’

Here are two mathematical examples.

Worked Exercise A73

For each of the following relations on the set \mathbb{R} , state whether the relation is reflexive, symmetric and transitive, briefly justifying your answers, and hence state whether the relation is an equivalence relation.

(a) $=$ (b) $<$

Solution

(a) **E1** The relation $=$ is reflexive, since, for all $x \in \mathbb{R}$, $x = x$.

E2 It is also symmetric, since, for all $x, y \in \mathbb{R}$, if $x = y$, then $y = x$.

E3 Finally, it is transitive, since, for all $x, y, z \in \mathbb{R}$, if $x = y$ and $y = z$, then $x = z$.

Hence this relation is an equivalence relation.

(b) **E1** The relation $<$ is not reflexive, since, for example, it is not true that $1 < 1$.

E2 Nor is it symmetric, since, for example, $1 < 2$ but it is not true that $2 < 1$.

E3 However, it is transitive, since, for all $x, y, z \in \mathbb{R}$, if $x < y$ and $y < z$, then $x < z$.

Since this relation is not reflexive (or symmetric), it is not an equivalence relation.

Notice that the statements that you need to prove to show that a relation is reflexive, symmetric or transitive, which are given in the definition in the box shortly before Worked Exercise A72, start with the words ‘For all’ and are therefore *universal statements*. So to show that a relation \sim on a set X is reflexive, for example, you must show that $x \sim x$ for all elements x in X : it is not enough to show that there exists an element x in X such that $x \sim x$. To show that a relation \sim on a set X is *not* reflexive, you just have to show that there is a counterexample – that is, an element x in X such that $x \not\sim x$.

Similarly, to show that a relation \sim on a set X is symmetric, you must prove that $x \sim y \implies y \sim x$ for every $x, y \in X$, while to show that it is *not* symmetric, you just have to show that there is a counterexample, that is, a pair $x, y \in X$ for which this property does not hold. Analogous statements hold for the transitive property, involving triples $x, y, z \in X$.

Here is a worked exercise involving two mathematical relations that are more complicated than $=$ and $<$. You met these two relations earlier in this subsection.

Worked Exercise A74

For each relation below, determine whether it has the reflexive, symmetric and transitive properties, and hence state whether it is an equivalence relation.

- (a) The relation \sim defined on \mathbb{C} by

$$z_1 \sim z_2 \quad \text{if } |z_1 - z_2| \leq 4.$$

- (b) The relation \sim defined on \mathbb{R} by

$$x \sim y \quad \text{if } x - y \text{ is an integer.}$$

Solution

- (a) **E1** Let $z \in \mathbb{C}$. Then

$$|z - z| = 0 \leq 4,$$

so $z \sim z$. Thus \sim is reflexive.

- E2** Let $z_1, z_2 \in \mathbb{C}$, and suppose that $z_1 \sim z_2$. Then $|z_1 - z_2| \leq 4$, so

$$|z_2 - z_1| = |z_1 - z_2| \leq 4.$$

Hence $z_2 \sim z_1$. Thus \sim is symmetric.

- E3** The relation \sim is not transitive, as demonstrated by the example $z_1 = 0$, $z_2 = 3$, $z_3 = 6$ (illustrated in Figure 4):

$$|z_1 - z_2| = |0 - 3| = |-3| = 3 \leq 4, \quad \text{so } z_1 \sim z_2,$$

$$|z_2 - z_3| = |3 - 6| = |-3| = 3 \leq 4, \quad \text{so } z_2 \sim z_3,$$

but

$$|z_1 - z_3| = |0 - 6| = |-6| = 6 > 4, \quad \text{so } z_1 \not\sim z_3.$$

Since \sim is not transitive, it is not an equivalence relation.

- (b) **E1** Let $x \in \mathbb{R}$. Then $x - x = 0$, which is an integer. Thus \sim is reflexive.

- E2** Let $x, y \in \mathbb{R}$, and suppose that $x \sim y$. Then $x - y$ is an integer, say

$$x - y = k,$$

where $k \in \mathbb{Z}$. It follows that

$$y - x = -(x - y) = -k,$$

which is an integer. Hence $y \sim x$. Thus \sim is symmetric.

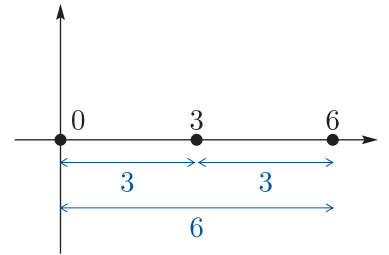




Figure 4 Some distances in the complex plane

E3 Let $x, y, z \in \mathbb{R}$, and suppose that $x \sim y$ and $y \sim z$. Then $x - y$ and $y - z$ are integers, say

$$x - y = k \quad \text{and} \quad y - z = m,$$

where $k, m \in \mathbb{Z}$.

 We notice that $(x - y) + (y - z) = x - z$. 

We have

$$x - z = x - y + y - z = k + m,$$

which is an integer. Hence $x \sim z$. Thus \sim is transitive.

Since \sim is reflexive, symmetric and transitive, it is an equivalence relation.

Here is a similar exercise for you to try. In part (e), note that in this unit we will take the definition of **parallel** to be ‘in the same direction as’. Thus any line is parallel to itself. In fact the word *parallel* may be defined to have either of two possible meanings: the meaning just mentioned, and the one given in Unit A1 in which two lines are *parallel* if they never meet. Both definitions are accepted in mathematics; the only difference between them is that with the definition in Unit A1 a line is not parallel to itself.

Part (f) of the exercise involves the *integer part* of a real number. For any real number x , the **integer part** of x (also called the **floor** of x), denoted by $\lfloor x \rfloor$, is the largest integer that is less than or equal to x . (You will meet this again in your study of functions in Unit A4 *Real functions, graphs and conics*.) For example, $\lfloor 4.3 \rfloor = 4$, $\lfloor -4.3 \rfloor = -5$ and $\lfloor 4 \rfloor = 4$. So, for any real number x , the integer part $\lfloor x \rfloor$ of x is obtained by rounding down to the nearest integer; the rounding is always *down*, no matter whether x is positive or negative.

Exercise A130

For each relation below, determine whether it has the reflexive, symmetric and transitive properties, and hence state whether it is an equivalence relation.

(a) The relation \sim defined on \mathbb{Z} by

$$m \sim n \quad \text{if } m - n \text{ is even.}$$

(b) The relation \sim defined on \mathbb{Z} by

$$m \sim n \quad \text{if } m - n \text{ is odd.}$$

(c) The relation \sim defined on \mathbb{Z} by

$$m \sim n \quad \text{if } m^2 + n^2 \text{ is even.}$$

(d) The relation \sim defined on \mathbb{C} by

$$z_1 \sim z_2 \quad \text{if } |z_1| = |z_2|.$$

(e) The relation \sim defined on the set of all lines in the plane by

$$l_1 \sim l_2 \quad \text{if the lines } l_1 \text{ and } l_2 \text{ are parallel.}$$

(f) The relation \sim defined on \mathbb{R} by

$$x \sim y \quad \text{if } \lfloor x - y \rfloor = 0.$$

You have already met an important family of equivalence relations in Unit A2. Let n be any integer greater than 1, and consider the relation *is congruent modulo n to* on the set \mathbb{Z} . As you have seen, this relation is usually denoted by the special symbol \equiv , and we usually also include ‘(mod n)’ to make it clear which value of n we are working with. For example, with $n = 7$, the statement

$$1 \equiv 8 \pmod{7}$$

is true, and the statement

$$1 \equiv 12 \pmod{7}$$

is false.

You saw in Unit A2 that the reflexive, symmetric and transitive properties hold for congruence modulo n ; these properties are the first three properties in Theorem A10 in that unit. So we have the following theorem.

Theorem A15

For any integer $n > 1$, congruence modulo n is an equivalence relation on \mathbb{Z} .

Very roughly, you can think of any equivalence relation as a relation that defines some kind of ‘equivalence’ on the objects in the set on which the relation is defined.

For example, with the equivalence relation *was born in the same year as* on a set of people, two people are ‘equivalent’ if they were born in the same year. Imagine that you are selecting people to take part in a survey, and the only selection criterion is that you need to select ten people born in each year from 1950 to 1999. Then, as far as selecting people for the survey is concerned, you would consider two people to be ‘equivalent’ if they were born in the same year. For instance, if Ashok and Becky were both born in 1992, then it doesn’t matter which of them you select: they are equivalent.

Here are two mathematical examples. First, with the equivalence relation *is equal to* on the set \mathbb{R} , two real numbers are ‘equivalent’ if they are equal. This is a very strict type of equivalence, where two objects are ‘equivalent’ only if they are exactly the same (though they might be written differently, such as $\frac{1}{2}$, $\frac{3}{6}$ and 0.5).

Second, with the equivalence relation in Exercise A130(e), two lines in the plane are ‘equivalent’ if they are parallel. This equivalence between lines might be useful if we were interested only in the directions of lines and not in their positions in the plane.

With the equivalence relation congruence modulo n , two integers are ‘equivalent’ if they have the same remainder on division by n . We use this type of equivalence when we carry out modular arithmetic.

Finally in this subsection, here is an interesting ‘spot the error’ exercise. It involves an incorrect proof that appears to show that if a relation is both symmetric and transitive, then it is also reflexive. If this were true, then we could define an equivalence relation to be a relation that is symmetric and transitive – we could omit the condition that it must also be reflexive. However, it is not true, as you are asked to show in the exercise. The error in the proof is very subtle. It highlights just how careful we need to be in mathematical arguments.

Exercise A131

Consider the following incorrect claim and incorrect proof.

Claim (incorrect)

Let \sim be a relation on a set X . If \sim is symmetric and transitive, then \sim is also reflexive.

Proof (incorrect) Suppose that \sim is symmetric and transitive. We will show that \sim is then also reflexive. Let $x \in X$. We have to show that $x \sim x$. Let y be an element of X such that $x \sim y$. Then, since \sim is symmetric, we have $y \sim x$. Since $x \sim y$ and $y \sim x$, and \sim is transitive, we have $x \sim x$, as required. Thus \sim is reflexive. ■

- (a) Show that the claim is incorrect by demonstrating that the relation \sim defined on \mathbb{R} by

$$x \sim y \quad \text{if } xy > 0$$

is a counterexample. That is, you have to show that this relation \sim is symmetric and transitive, but not reflexive.

- (b) Try to spot the error in the given proof. (Do not worry if you cannot spot it, as it is subtle, but be impressed with yourself if you can! Make sure to look at the answer.)

4.2 Equivalence classes

We now look at the idea of an *equivalence class*. This idea is associated only with equivalence relations, not with relations in general.

Definition

Let \sim be an equivalence relation on a set X , and let $x \in X$. Then the **equivalence class** of x , denoted by $\llbracket x \rrbracket$, is the set

$$\llbracket x \rrbracket = \{y \in X : x \sim y\}.$$

In other words, $\llbracket x \rrbracket$ is the set of all the elements in X that are related to x by the equivalence relation; that is, it is the set of all the elements in X that are equivalent to x , where the equivalence is given by the equivalence relation. Notice that $\llbracket x \rrbracket$ includes the element x itself, because for an equivalence relation we have $x \sim x$.

For example, consider the equivalence relation *was born in the same year as* on a set of people. The equivalence class of a particular person is the set of people who were born in the same year as that person, including the person themselves.

As a mathematical example, consider the equivalence relation on the set of lines in the plane defined by

$$l_1 \sim l_2 \quad \text{if the lines } l_1 \text{ and } l_2 \text{ are parallel.}$$

You saw that this relation is an equivalence relation in Exercise A130(e). Consider any particular line l in the plane. Then the equivalence class $\llbracket l \rrbracket$ of l is the set of all the lines in the plane that are parallel to l , including l itself.

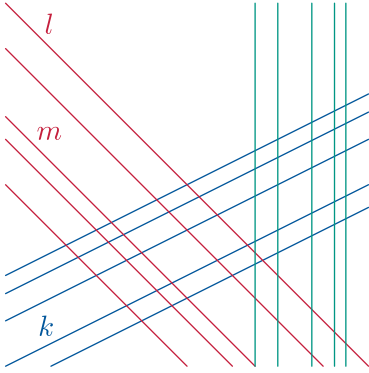


Figure 5 Lines in the plane

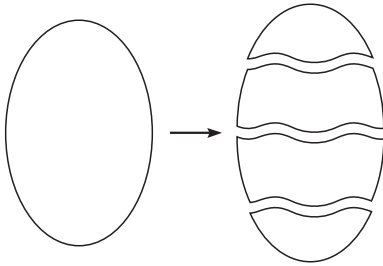


Figure 6 Partitioning a set

Let us think about this example a little more. Consider a particular line l , as illustrated in Figure 5. Notice if you choose any line, say m , that lies in the equivalence class $\llbracket l \rrbracket$ of l , then $\llbracket m \rrbracket$ and $\llbracket l \rrbracket$ are in fact the *same set*. On the other hand, if you choose a line, say k , that is *not* in the equivalence class $\llbracket l \rrbracket$ of the original line l , then not only are the two sets $\llbracket k \rrbracket$ and $\llbracket l \rrbracket$ different sets, but in fact they are *disjoint* sets. (Remember that two sets are said to be **disjoint** if they have no elements in common.)

In fact, you can see that essentially what has happened here is that the set of all the lines in the plane has been split into a collection of subsets, with each subset consisting of all the lines in a particular direction.

So the equivalence classes of this particular equivalence relation split the set on which the relation is defined into a collection of subsets, such that each pair of these subsets is disjoint. Such a collection of subsets is known as a *partition* of the set, as defined below and illustrated in Figure 6.

Definitions

A collection of non-empty subsets of a set is a **partition** of the set if every pair of subsets in the collection is disjoint and the union of all the subsets in the collection is the whole set.

We say that such a collection of subsets **partitions** the set.

In other words, a collection of non-empty subsets of a set is a partition of the set if *every* element of the set belongs to *exactly one* of the subsets in the collection.

In fact, for *every* equivalence relation, its equivalence classes form a partition of the set on which the relation is defined, as stated and proved below.

Theorem A16

The equivalence classes of an equivalence relation on a set X form a partition of the set X .

Proof First, since every element x of X belongs to an equivalence class, namely its own equivalence class $\llbracket x \rrbracket$, the union of the equivalence classes of \sim is the whole set X .

To prove that the equivalence classes of \sim partition the set X , the other property that we have to show is that if x and y are any elements of X , then their equivalence classes $\llbracket x \rrbracket$ and $\llbracket y \rrbracket$ are either the *same* subset of X , or *disjoint* subsets of X . We can prove this as follows.

Let x and y be elements of X , and suppose that $\llbracket x \rrbracket$ and $\llbracket y \rrbracket$ are *not* disjoint, that is, they have at least one element in common, say z . We will show that $\llbracket x \rrbracket$ and $\llbracket y \rrbracket$ must then be the same set, that is, $\llbracket x \rrbracket = \llbracket y \rrbracket$.

🔗 To do this, we use the strategy for proving that two sets are equal given in Unit A1: we show that each set is a subset of the other. 🔗

First we show that $\llbracket x \rrbracket \subseteq \llbracket y \rrbracket$. Suppose that $a \in \llbracket x \rrbracket$; we have to show that $a \in \llbracket y \rrbracket$. Since both a and z are in $\llbracket x \rrbracket$, we know that $x \sim a$ and $x \sim z$. Hence (since the relation \sim is symmetric and transitive) we have $a \sim z$. But we also know that $y \sim z$, because $z \in \llbracket y \rrbracket$, so (again since \sim is symmetric and transitive) it follows that $y \sim a$. Hence $a \in \llbracket y \rrbracket$, as claimed.

We can show in the same way that $\llbracket y \rrbracket \subseteq \llbracket x \rrbracket$ (we interchange the roles of x and y in the proof that $\llbracket x \rrbracket \subseteq \llbracket y \rrbracket$).

Hence $\llbracket x \rrbracket = \llbracket y \rrbracket$. This completes the proof. ■

The proposition below was proved as part of the proof of Theorem A16 above, and you saw it illustrated for a particular equivalence relation (the one involving lines in the plane) near the start of this subsection. It is an important fact to keep in mind when you are working with equivalence classes.

Proposition A17

The equivalence classes of an equivalence relation on a set X have the following property: if x and y are elements of X , then their equivalence classes $\llbracket x \rrbracket$ and $\llbracket y \rrbracket$ are either equal sets or disjoint sets.

If you think about an equivalence relation as defining a type of ‘equivalence’, then Theorem A16 seems true intuitively. Each equivalence class is a subset of elements that are all ‘equivalent’ to each other. Each element lies in such a class, and each element is not equivalent to any element outside its own class.

As an example of Theorem A16, consider the equivalence relation *was born in the same year as* on a set of people. The equivalence class of each person is the set of people born in the same year as that person. So the whole set of people is partitioned into a set of classes: the class of people born in 1966, the class of people born in 1992, the class of people born in 2001, and so on. Each person belongs to one of these classes, and each pair of the classes is disjoint.

As a mathematical example of Theorem A16, consider the equivalence relation *is equal to* on \mathbb{R} . Consider any number $x \in \mathbb{R}$. Since $x = y$ only if y is the same number as x , the equivalence class of the real number x contains only the number x itself. So each element lies in a single-element equivalence class, as illustrated in Figure 7. For example, $\llbracket 0 \rrbracket = \{0\}$, $\llbracket 1 \rrbracket = \{1\}$, and so on.

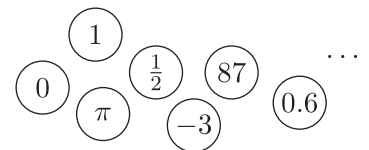


Figure 7 Some equivalence classes of ‘is equal to’

As another mathematical example of Theorem A16, consider the equivalence relation *congruence modulo 5* defined on \mathbb{Z} . The equivalence class of 0 is the subset of \mathbb{Z} containing all the integers that are congruent to 0 modulo 5. Similarly, the equivalence class of 1 is the subset of \mathbb{Z} containing all the integers that are congruent to 1 modulo 5, and so on. That is,

$$\begin{aligned}\llbracket 0 \rrbracket &= \{\dots, -10, -5, 0, 5, 10, 15, \dots\}, \\ \llbracket 1 \rrbracket &= \{\dots, -9, -4, 1, 6, 11, 16, \dots\}, \\ \llbracket 2 \rrbracket &= \{\dots, -8, -3, 2, 7, 12, 17, \dots\}, \\ \llbracket 3 \rrbracket &= \{\dots, -7, -2, 3, 8, 13, 18, \dots\}, \\ \llbracket 4 \rrbracket &= \{\dots, -6, -1, 4, 9, 14, 19, \dots\}.\end{aligned}$$

There are only five *distinct* equivalence classes since, for example, $\llbracket 5 \rrbracket$ is the same set as $\llbracket 0 \rrbracket$, and $\llbracket 6 \rrbracket$ is the same set as $\llbracket 1 \rrbracket$, and so on. The collection of five equivalence classes partitions the set \mathbb{Z} , as illustrated in Figure 8: every number in \mathbb{Z} belongs to one of the five classes, and the five classes are all disjoint from each other.

In general, congruence modulo n partitions the set \mathbb{Z} into n distinct equivalence classes.

Notice that an equivalence class of an equivalence relation may be a finite set or an infinite set, and that an equivalence relation may have finitely many equivalence classes or infinitely many equivalence classes.

The next worked exercise involves finding a particular equivalence class of another equivalence relation.

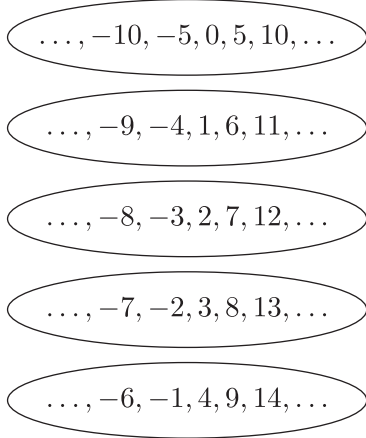


Figure 8 The five equivalence classes of congruence modulo 5

Worked Exercise A75

Find the equivalence class $\llbracket 3.7 \rrbracket$ of the equivalence relation defined on \mathbb{R} by

$$x \sim y \quad \text{if } x - y \text{ is an integer.}$$

(You saw that this relation is an equivalence relation in Worked Exercise A74(b).)

Solution

Apply the definition of an equivalence class, then try to express the resulting set in as simple a way as possible without using the symbol \sim , to make it clear what the elements of the set are.

We have

$$\begin{aligned}\llbracket 3.7 \rrbracket &= \{y \in \mathbb{R} : 3.7 \sim y\} \\ &= \{y \in \mathbb{R} : 3.7 - y \text{ is an integer}\} \\ &= \{y \in \mathbb{R} : 3.7 - y = k \text{ for some } k \in \mathbb{Z}\} \\ &= \{y \in \mathbb{R} : y = 3.7 - k \text{ for some } k \in \mathbb{Z}\}\end{aligned}$$

☁ The set of real numbers y such that $y = 3.7 - k$ for some integer k is the same as the set of real numbers y such that $y = 3.7 + k$ for some integer k . And we can write $3.7 + k$ as $k + 3.7$. ☁

$$= \{y \in \mathbb{R} : y = k + 3.7 \text{ for some } k \in \mathbb{Z}\}$$

☁ The set of real numbers y such that $y = k + 3.7$ for some integer k is, more simply, the set of numbers of the form $k + 3.7$ for some integer k . ☁

$$= \{k + 3.7 : k \in \mathbb{Z}\}$$

☁ Saying that an integer is of the form ‘some integer plus 3.7’ is the same as saying that it is of the form ‘some integer plus 0.7’. The latter is slightly simpler. ☁

$$= \{k + 0.7 : k \in \mathbb{Z}\}.$$

This set can also be written (less concisely) as

$$[3.7] = \{\dots, -2.3, -1.3, -0.3, 0.7, 1.7, 2.7, 3.7, \dots\}.$$

Exercise A132

Find the equivalence class $[1]$ of the equivalence relation \sim defined on \mathbb{Z} by

$$m \sim n \quad \text{if } m - n \text{ is even.}$$

(You saw that this relation is an equivalence relation in Exercise A130(a).)

If we want to find *all* the equivalence classes of an equivalence relation, then it often helps to start by finding a particular equivalence class, or a few particular equivalence classes, as demonstrated in the next worked exercise. This can help us to see what happens in general.

Worked Exercise A76

Let \sim be the equivalence relation defined on \mathbb{C} by

$$z_1 \sim z_2 \quad \text{if } |z_1| = |z_2|.$$

(You saw that this relation is an equivalence relation in Exercise A130(d).)

- (a) Find the equivalence classes $\llbracket 0 \rrbracket$ and $\llbracket i \rrbracket$.
- (b) Describe all the equivalence classes of \sim .

Solution

- (a) We have

$$\begin{aligned}\llbracket 0 \rrbracket &= \{z \in \mathbb{C} : 0 \sim z\} \\ &= \{z \in \mathbb{C} : |0| = |z|\} \\ &= \{z \in \mathbb{C} : |z| = 0\} \\ &= \{0\}.\end{aligned}$$

So $\llbracket 0 \rrbracket$ is the set containing the complex number 0 alone.

Similarly,

$$\begin{aligned}\llbracket i \rrbracket &= \{z \in \mathbb{C} : i \sim z\} \\ &= \{z \in \mathbb{C} : |i| = |z|\} \\ &= \{z \in \mathbb{C} : |z| = 1\}.\end{aligned}$$

So $\llbracket i \rrbracket$ is the set of all complex numbers of modulus 1.

- (b) In general, for any complex number z_0 , say, we have

$$\begin{aligned}\llbracket z_0 \rrbracket &= \{z \in \mathbb{C} : z_0 \sim z\} \\ &= \{z \in \mathbb{C} : |z_0| = |z|\} \\ &= \{z \in \mathbb{C} : |z| = |z_0|\}.\end{aligned}$$

So $\llbracket z_0 \rrbracket$ is the set of all complex numbers with the same modulus as z_0 .

If $|z_0| = r$, say, then

$$\llbracket z_0 \rrbracket = \{z \in \mathbb{C} : |z| = r\}.$$

This set forms the circle with centre the origin and radius r in the complex plane.

Hence the equivalence classes of \sim are the circles in the complex plane with centre the origin. (The origin is an equivalence class containing just the complex number 0; it can be thought of as a circle of radius 0.)

Some of the equivalence classes of the equivalence relation in Worked Exercise A76 are illustrated in Figure 9. They are the circles with centre the origin, together with the origin itself. Notice that, as expected, the equivalence classes partition the set on which the equivalence relation is defined.

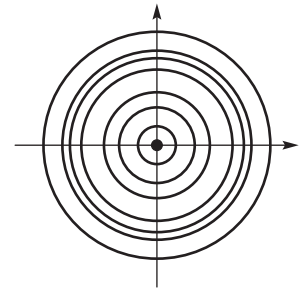


Figure 9 Some equivalence classes of the equivalence relation in Worked Exercise A76

Exercise A133

Determine all the equivalence classes of the equivalence relation \sim defined on \mathbb{Z} by

$$m \sim n \quad \text{if } m - n \text{ is even.}$$

(You saw that this relation is an equivalence relation in Exercise A130(a), and you were asked to find the equivalence class $\llbracket 1 \rrbracket$ of this relation in Exercise A132.)

Exercise A134

Let \sim be the relation defined on \mathbb{R} by

$$x \sim y \quad \text{if } \lfloor x \rfloor = \lfloor y \rfloor.$$

(Remember that $\lfloor x \rfloor$ denotes the integer part of x : the largest integer that is less than or equal to x ; for example $\lfloor 4.72 \rfloor = 4$.)

- Show that \sim is an equivalence relation.
- Determine the equivalence classes $\llbracket 1 \rrbracket$ and $\llbracket -4 \rrbracket$.
- Describe all the equivalence classes of \sim .

As a further exercise on equivalence classes, you are asked next to prove the converse of Theorem A16, namely that every partition of a set X gives rise to an equivalence relation on X whose equivalence classes are the subsets that make up the partition.

Exercise A135

Let X be a set, and suppose we are given a collection of non-empty subsets of X that forms a partition of X . Let \sim be the relation defined on X by

$$x \sim y \quad \text{if } x \text{ and } y \text{ belong to the same subset in the partition.}$$

Show that \sim is an equivalence relation on X .

Representatives of equivalence classes

You have seen that if \sim is an equivalence relation on a set X , and x and y are two elements of X such that $x \sim y$, then $\llbracket x \rrbracket = \llbracket y \rrbracket$. Thus, in general, there is more than one way to denote each equivalence class using the notation $\llbracket \cdot \rrbracket$: a class can be denoted by $\llbracket x \rrbracket$ where x is any one of its elements. For example, consider again the equivalence classes of the equivalence relation congruence modulo 5:

$$\begin{aligned}\llbracket 0 \rrbracket &= \{\dots, -10, -5, 0, 5, 10, 15, \dots\}, \\ \llbracket 1 \rrbracket &= \{\dots, -9, -4, 1, 6, 11, 16, \dots\}, \\ \llbracket 2 \rrbracket &= \{\dots, -8, -3, 2, 7, 12, 17, \dots\}, \\ \llbracket 3 \rrbracket &= \{\dots, -7, -2, 3, 8, 13, 18, \dots\}, \\ \llbracket 4 \rrbracket &= \{\dots, -6, -1, 4, 9, 14, 19, \dots\}.\end{aligned}$$

We can denote the first equivalence class here by $\llbracket 0 \rrbracket$, or by $\llbracket 5 \rrbracket$, or by $\llbracket -5 \rrbracket$, and so on. Similarly, we can denote the second equivalence class by $\llbracket 1 \rrbracket$, or by $\llbracket 6 \rrbracket$, or by $\llbracket -4 \rrbracket$, and so on; and similarly for the other equivalence classes.

When we are working with an equivalence relation, it is sometimes useful to choose a particular element x in each equivalence class and normally denote the class by $\llbracket x \rrbracket$. The element x that we choose is called a **representative** of the class.

For example, for the equivalence relation congruence modulo 5, whose equivalence classes are listed above, the most convenient representatives for the five classes are 0, 1, 2, 3 and 4.

In general, if \sim is an equivalence relation on a set X , then a set of elements of X that contains exactly one element from each equivalence class of \sim is called a **set of representatives** for the equivalence relation \sim . For example, $\{0, 1, 2, 3, 4\}$ is a set of representatives for congruence modulo 5.

More generally, for any integer $n \geq 2$, the equivalence relation congruence modulo n has n equivalence classes, and the most convenient set of representatives for them is $\{0, 1, 2, \dots, n-1\}$, as set out below.

$$\begin{aligned}\llbracket 0 \rrbracket &= \{\dots, -2n, -n, 0, n, 2n, \dots\}, \\ \llbracket 1 \rrbracket &= \{\dots, 1-2n, 1-n, 1, 1+n, 1+2n, \dots\}, \\ &\vdots \\ \llbracket n-1 \rrbracket &= \{\dots, -n-1, -1, n-1, 2n-1, 3n-1, \dots\}.\end{aligned}$$

In other words, the most convenient set of representatives for the equivalence relation congruence modulo n is the set $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$, which you worked with in Subsection 3.3 of Unit A2. The definitions of the modular operations $+_n$ and \times_n can be rephrased in terms of the equivalence classes of the equivalence relation congruence modulo n , as follows.

For all $a, b \in \mathbb{Z}_n$,

$a +_n b$ is the integer in \mathbb{Z}_n that lies in the class $\llbracket a + b \rrbracket$,

$a \times_n b$ is the integer in \mathbb{Z}_n that lies in the class $\llbracket a \times b \rrbracket$.

For example, in \mathbb{Z}_5 ,

$$3 +_5 4 = 2,$$

because $3 + 4 = 7$ and the equivalence class $\llbracket 7 \rrbracket$ of congruence modulo 5 contains the element 2 of \mathbb{Z}_5 .

Exercise A136

Use the definitions of $+_n$ and \times_n above to calculate $4 +_5 4$ and $3 \times_5 4$, writing out the details of your working.

As another example of using representatives for equivalence classes, consider again the equivalence relation \sim defined on \mathbb{C} by

$$z_1 \sim z_2 \quad \text{if } |z_1| = |z_2|.$$

The equivalence classes of this equivalence relation were found in Worked Exercise A76 to be all the sets of the form

$$\{z \in \mathbb{C}: |z| = r\},$$

where $r \in \mathbb{R}$. That is, they are the circles in the complex plane with centre the origin, including the origin itself as a ‘circle of radius 0’.

Consider the particular equivalence class

$$\{z \in \mathbb{C} : |z| = 4\},$$

that is, the circle of radius 4, which is shown in Figure 10(a). This class contains the complex numbers 4, $-4i$ and $-2\sqrt{2}(1+i)$, for example, since all these complex numbers have modulus 4. So we could denote this equivalence class by any of $\llbracket 4 \rrbracket$, $\llbracket -4i \rrbracket$ or $\llbracket -2\sqrt{2}(1+i) \rrbracket$, for example. We might decide that it is convenient to choose the representative 4, and denote the class by $\llbracket 4 \rrbracket$. In general, the equivalence class

$$\{z \in \mathbb{C} : |z| = r\},$$

of this equivalence relation contains the element r and so can be denoted by $\llbracket r \rrbracket$. Some examples of this choice of representatives are shown in Figure 10(b).

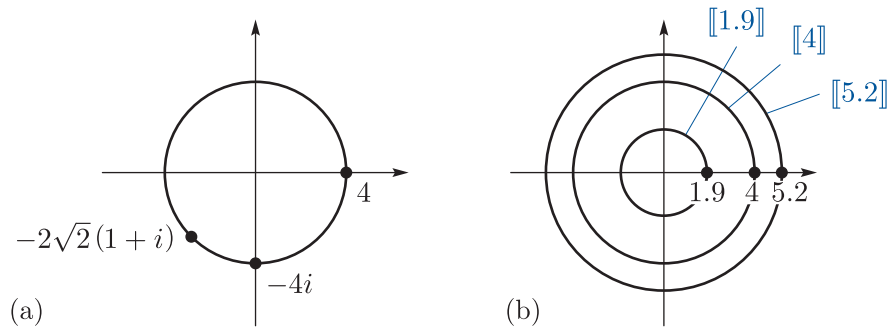


Figure 10 For the equivalence relation given by $z_1 \sim z_2$ if $|z_1| = |z_2|$:
(a) a particular equivalence class (b) some equivalence classes with representatives

A set of complex numbers that contains exactly one element from each equivalence class of the equivalence relation \sim is the set $[0, \infty)$, the set of all non-negative real numbers. So $[0, \infty)$ is a set of representatives for \sim .

Exercise A137

Describe a set of representatives for each of the following equivalence relations.

- (a) The relation \sim defined on \mathbb{Z} by

$$m \sim n \quad \text{if } m - n \text{ is even.}$$

(You saw that \sim is an equivalence relation in Exercise A130(a), and you were asked to find its equivalence classes in Exercise A133.)

- (b) The relation \sim defined on \mathbb{R} by

$$x \sim y \quad \text{if } \lfloor x \rfloor = \lfloor y \rfloor.$$

(You were asked to show that \sim is an equivalence relation, and find its equivalence classes, in Exercise A134.)

Congruence modulo 2π

To end this subsection we look at an equivalence relation that is similar to congruence modulo n on \mathbb{Z} , but which is defined on \mathbb{R} rather than \mathbb{Z} , and in which the modulus is 2π , rather than an integer n . You will see that this equivalence relation enables us to express concisely some results about complex numbers.

This relation is the relation \sim defined on \mathbb{R} by

$$x \sim y \quad \text{if } x - y = 2\pi k \text{ for some integer } k.$$

We begin by showing that this relation actually is an equivalence relation.

E1 Let $x \in \mathbb{R}$. Then $x - x = 0 = 2\pi \times 0$, so $x \sim x$. Thus \sim is reflexive.

E2 Let $x, y \in \mathbb{R}$ and suppose that $x \sim y$. Then

$$x - y = 2\pi k$$

for some integer k . Hence

$$y - x = 2\pi(-k).$$

Since $-k$ is an integer, this shows that $y \sim x$. Thus \sim is symmetric.

E3 Let $x, y, z \in \mathbb{R}$ and suppose that $x \sim y$ and $y \sim z$. Then

$$x - y = 2\pi j \quad \text{and} \quad y - z = 2\pi k$$

for some integers j and k . Hence

$$x - z = x - y + y - z = 2\pi(j + k).$$

Since $j + k$ is an integer, this shows that $x \sim z$. Thus \sim is transitive.

Since \sim is reflexive, symmetric and transitive, it is an equivalence relation.

The equivalence relation \sim above is known as **congruence modulo 2π** .

For this equivalence relation, we can use notation similar to the notation that we use for congruence modulo n . That is, rather than writing

$$x \sim y,$$

we can write

$$x \equiv y \pmod{2\pi}.$$

For example,

$$\frac{9\pi}{2} \equiv \frac{\pi}{2} \pmod{2\pi},$$

because

$$\frac{9\pi}{2} - \frac{\pi}{2} = 2 \times 2\pi.$$

You have seen that congruence modulo n on \mathbb{Z} corresponds to modular arithmetic on the set \mathbb{Z}_n , which is a set of representatives of the equivalence classes of congruence modulo n . In a similar way, congruence modulo 2π on \mathbb{R} corresponds to modular arithmetic on a set of representatives of the equivalence classes of congruence modulo 2π . The equivalence classes of \sim are the sets of the form

$$[x] = \{x + 2n\pi : n \in \mathbb{Z}\},$$

where $x \in \mathbb{R}$. For example, one equivalence class is

$$[0] = \{\dots, -4\pi, -2\pi, 0, 2\pi, 4\pi, \dots\},$$

and another is

$$\left[\frac{\pi}{2}\right] = \left\{\dots, -\frac{7\pi}{2}, -\frac{3\pi}{2}, \frac{\pi}{2}, \frac{5\pi}{2}, \frac{9\pi}{2}, \dots\right\}.$$

A suitable set of representatives for the equivalence classes is the interval $(-\pi, \pi]$, since every equivalence class has exactly one representative in this interval. Other intervals can be used, for example $[0, 2\pi)$, but $(-\pi, \pi]$ is useful as it corresponds to our definition of the principal argument of a complex number.

We define modular operations $+_{2\pi}$ and $\times_{2\pi}$ on the interval $(-\pi, \pi]$ as follows. For all $x, y \in (-\pi, \pi]$,

$x +_{2\pi} y$ is the real number in $(-\pi, \pi]$ that lies in the class $[x + y]$,

$x \times_{2\pi} y$ is the real number in $(-\pi, \pi]$ that lies in the class $[xy]$.

For example,

$$\pi +_{2\pi} \frac{\pi}{2} = -\frac{\pi}{2},$$

since $\pi + \frac{\pi}{2} = \frac{3\pi}{2}$ and $\left[\frac{3\pi}{2}\right]$ contains the element $-\frac{\pi}{2}$ of $(-\pi, \pi]$. This type of modular arithmetic is effectively what we do when we find the *principal* argument of a complex number arising from some calculation.

Recall that the principal argument of a complex number z is denoted by $\text{Arg } z$. Arithmetic modulo 2π on the interval $(-\pi, \pi]$ gives us a concise way to express some results about complex numbers that involve principal arguments. For example, you saw in Unit A2 that, if z_1 and z_2 are any two complex numbers, then $\text{Arg } z_1 + \text{Arg } z_2$ is an argument of $z_1 z_2$, but is not necessarily the principal argument. The principal argument is $\text{Arg } z_1 +_{2\pi} \text{Arg } z_2$, so we can now state that

$$\text{Arg}(z_1 z_2) = \text{Arg } z_1 +_{2\pi} \text{Arg } z_2.$$

You have now seen what congruence modulo 2π means. For any integer $r \in \mathbb{R}$, we can define congruence modulo r on \mathbb{R} in a similar way to the way that congruence modulo 2π is defined, and it can be checked that this relation is an equivalence relation in a similar way to the argument above. In fact, the equivalence relation in Worked Exercise A74(b) is congruence modulo 1 on \mathbb{R} . However, congruence modulo 2π is particularly useful, for the reasons you saw above.

Summary

In this unit you have been working with the bricks and mortar from which mathematics is built – the statements that express mathematical ideas and the proofs that establish which statements are true.

You have met different types of mathematical statements and seen how they can be combined and negated to make new statements. You have encountered several different methods of proof – some direct, such as the Principle of Mathematical Induction, and others indirect, such as proof by contradiction and proof by contraposition. You have also practised writing your own proofs and learned how to critically analyse mathematical arguments.

Skills such as these are not acquired easily, so do not be discouraged if you found some parts of this unit rather hard. There will be many more opportunities to read and write proofs as you work through the remaining units in this module, so your skills will develop as you continue your studies.

Finally, you have been introduced to the important topic of an equivalence relation on a set – a precise way of defining which elements of a set we regard as equivalent or ‘the same’. You will make extensive use of equivalence relations in the group theory units of this module.

Learning outcomes

After working through this unit, you should be able to:

- understand what is asserted by various types of mathematical statements, in particular *implications* and *equivalences*
- negate a mathematical statement, including *universal* and *existential* statements
- produce simple proofs of various types, including *direct* proofs, proofs by *induction*, by *contradiction* and by *contraposition*
- disprove a universal statement by providing a *counterexample*
- read and understand the logical structure of more complex proofs
- critically analyse a mathematical argument to identify, explain and rectify mathematical errors
- explain the meanings of a *relation* defined on a set, an *equivalence relation* and a *partition* of a set
- determine whether a relation defined on a set is an equivalence relation by checking the *reflexive*, *symmetric* and *transitive properties*
- understand that an equivalence relation partitions a set into *equivalence classes*, and determine the equivalence classes for an equivalence relation.

Solutions to exercises

Solution to Exercise A101

(a) This is a mathematical statement. Whether the statement is true or false depends on the value of the variable n , so the statement is a variable proposition.

(b) This assertion is not a mathematical statement, as the property of ‘being small’ has not been defined mathematically, and so it is not precise enough.

(c) Since $\{1, 2, 3, 4\}$ is not an integer, it cannot be even or odd. Therefore this assertion is neither true nor false, and so it is not a mathematical statement.

(d) This is a mathematical statement (a false one). It contains no variable, and so is not a variable proposition.

Solution to Exercise A102

(a) The negation can be expressed as

$$x = \frac{3}{5} \text{ is not a solution of the equation } 3x + 5 = 0.$$

(b) The negation can be expressed as

The equation $n^2 + n - 2 = 0$ does not have exactly two solutions

or, more precisely, as

The equation $n^2 + n - 2 = 0$ has either no solution, exactly one solution or more than two solutions.

Solution to Exercise A103

(a) The negation is ‘it is not the case that both x and y are integers’; that is, ‘at least one of x or y is not an integer’. Some equivalent formulations of this negation are

either x or y is not an integer,

or

$$x \notin \mathbb{Z} \text{ or } y \notin \mathbb{Z}.$$

(b) The statement is equivalent to the conjunction ‘ m is even and n is odd’. The negation can be expressed as

m is odd or n is even.

(c) The statement is equivalent to the disjunction ‘ m is odd or n is odd’. The negation can be expressed as

the integers m and n are both even.

(d) The negation can be expressed as

$$A \neq \emptyset \text{ and } B \neq \emptyset.$$

Solution to Exercise A104

(a) The statement can be rewritten as

$$\text{if } x^2 - 2x + 1 = 0, \text{ then } (x - 1)^2 = 0.$$

This is true.

(b) The statement can be rewritten as

$$\text{if } n \text{ is odd, then } n^3 \text{ is odd.}$$

This is true.

(c) The statement can be rewritten as

if a given integer is divisible by 3, then it is also divisible by 6.

This is false.

(d) The statement can be rewritten as

$$\text{if } x > 2, \text{ then } x > 4.$$

This is false.

(e) The statement can be rewritten as

$$\text{if } x \leq 0, \text{ then } x^3 \leq 0.$$

This is true.

Solution to Exercise A105

(a) The negation is

m and n are odd, and $m + n$ is not odd,

that is,

m and n are odd, and $m + n$ is even.

- (b) The negation of ' $A \cup B = \emptyset$ or $B - A = \emptyset$ ' is
 $A \cup B \neq \emptyset$ and $B - A \neq \emptyset$.

Thus the negation of the implication is

$$A = \emptyset, \text{ and } A \cup B \neq \emptyset \text{ and } B - A \neq \emptyset.$$

Solution to Exercise A106

- (a) The converse is
 if $m + n$ is even, then m and n are both odd.

The given implication is true, and its converse is false.

- (b) The converse is
 if $m + n$ is odd, then one of the pair m, n is even and the other is odd.

The given implication and its converse are both true.

Solution to Exercise A107

- (a) The converse is
 if at least one of m or n is even, then mn is even.

The contrapositive is

$$\text{if both } m \text{ and } n \text{ are odd, then } mn \text{ is odd.}$$

The converse is true, and so is the contrapositive.
 (Since the contrapositive is true, the original statement is also true).

- (b) The converse is
 if q divides m or q divides n , then q divides the product mn .

The contrapositive is

$$\text{if } q \text{ divides neither } m \text{ nor } n, \text{ then } q \text{ does not divide the product } mn.$$

The converse is true, but the contrapositive (and hence the original statement) is false.

Solution to Exercise A108

- (a) The two implications are 'if the product mn is odd, then both m and n are odd', and 'if both m and n are odd, then the product mn is odd'. Both implications are true, so the equivalence is true.

- (b) The two implications are 'if the product mn is even, then both m and n are even', and 'if both m and n are even, then the product mn is even'. The first implication is false, and the second is true. As at least one implication is false, the equivalence is false.

Solution to Exercise A109

- (a) The negation is
 it is not the case that there is a real number x such that $\cos x = x$;

that is,

$$\text{there is no real number } x \text{ such that } \cos x = x.$$

Another way of expressing this negation is

$$\text{for all real numbers } x, \cos x \neq x.$$

- (b) The negation can be expressed as
 there is no integer that is divisible by 3 but not by 6,

or, alternatively,

$$\text{every integer that is divisible by 3 is also divisible by 6.}$$

- (c) The negation can be expressed as
 there is a real number x that does not satisfy the inequality $x^2 \geq 0$,

or, alternatively,

$$\text{there is a real number } x \text{ such that } x^2 < 0.$$

Solution to Exercise A110

- (a) Suppose that n is an even integer. Then $n = 2k$, where k is an integer, so

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2).$$

Since $2k^2$ is an integer, this proves that n^2 is even, as required.

- (b) Let m and n be multiples of k . Then $m = ka$ and $n = kb$, where a and b are integers. Hence

$$m + n = ka + kb = k(a + b).$$

Since $a + b$ is an integer, we deduce that $m + n$ is a multiple of k , as required.

(c) Suppose that one of the pair m, n is even and the other is odd. Then one of them is equal to $2k$ and the other to $2l + 1$, for some integers k and l . Then

$$m + n = 2k + (2l + 1) = 2(k + l) + 1.$$

Since $k + l$ is an integer, this shows that $m + n$ is odd.

(d) Let n be a positive integer. We note that

$$n^2 + n = n(n + 1).$$

Either n or $n + 1$ must be even, so their product $n^2 + n$ is even, as required.

(Alternatively, the implication can be proved by considering two separate cases: the case where n is even, and the case where n is odd. However, the proof above is shorter and simpler.)

Solution to Exercise A111

The problem lies in the step

$$x + 1 \leq 0 \implies (x + 1)^2 \leq 0.$$

This implication is false: take, for example, $x = -2$. The writer of the deduction seems to have used an incorrect assumption that an inequality is preserved by squaring its two sides, that is, that for real numbers a and b

$$a \leq b \implies a^2 \leq b^2.$$

(This implication only holds under the additional assumption that $a \geq 0$.)

Solution to Exercise A112

The problem with this argument is that it starts by assuming the statement to be proved ($|z_1| = |z_2|$) and uses it to deduce a second statement that is known to be true ($5 = 5$).

Deducing a true statement Q from a statement P does not tell us that P is true, so the truth of the second statement provides no information on the truth of the original statement.

Below is a correct proof that shows that each side of the equality to be proved is equal to the same value.

Since $z_1 = 1 + 2i$, we have

$$\begin{aligned} |z_1| &= \sqrt{1^2 + 2^2} \\ &= \sqrt{5}. \end{aligned}$$

Since $z_2 = \sqrt{3} - i\sqrt{2}$, we have

$$\begin{aligned} |z_2| &= \sqrt{(\sqrt{3})^2 + (-\sqrt{2})^2} \\ &= \sqrt{3 + 2} \\ &= \sqrt{5}. \end{aligned}$$

Therefore $|z_1| = \sqrt{5}$ and $|z_2| = \sqrt{5}$, so $|z_1| = |z_2|$ as required.

(An alternative, but less obvious, proof starts with the left-hand side of the equality to be proved and shows directly that it is equal to the right-hand side.

$$\begin{aligned} |z_1| &= \sqrt{1^2 + 2^2} \\ &= \sqrt{5} \\ &= \sqrt{3 + 2} \\ &= \sqrt{(\sqrt{3})^2 + (-\sqrt{2})^2} \\ &= |z_2|. \end{aligned}$$

Therefore $|z_1| = |z_2|$, as required.)

Solution to Exercise A113

(a) Assume that n is even. Then $n = 2k$ for some integer k , and so

$$\begin{aligned} n + 8 &= 2k + 8 \\ &= 2(k + 4). \end{aligned}$$

Since $k + 4$ is an integer, this shows that $n + 8$ is even. So

$$n \text{ is even} \implies n + 8 \text{ is even}.$$

Now assume that $n + 8$ is even. Then $n + 8 = 2k$ for some integer k , and so

$$\begin{aligned} n &= 2k - 8 \\ &= 2(k - 4). \end{aligned}$$

Since $k - 4$ is an integer, this shows that n is even. So

$$n + 8 \text{ is even} \implies n \text{ is even}.$$

Hence $n \text{ is even} \iff n + 8 \text{ is even}$.

(b) Assume that $A \subseteq A \cap B$, and let x be such that $x \in A$. Since $A \subseteq A \cap B$, it follows that $x \in A \cap B$, so, in particular, $x \in B$. Therefore $A \subseteq B$. So

$$A \subseteq A \cap B \implies A \subseteq B.$$

Now assume that $A \subseteq B$, and let x be such that $x \in A$. Then, since $A \subseteq B$, it follows that $x \in B$, and so $x \in A \cap B$. Hence $A \subseteq A \cap B$. So

$$A \subseteq B \implies A \subseteq A \cap B.$$

Hence $A \subseteq A \cap B \iff A \subseteq B$.

Solution to Exercise A114

The initial explanation of how to find a suitable integer is not a necessary part of the solution: it is included to show a possible way to find the example.

The condition $3^n > 9^n$ is equivalent to

$$\frac{3^n}{9^n} = \left(\frac{1}{3}\right)^n > 1.$$

This condition is satisfied by negative values of n , for example $n = -1$.

Let $n = -1$. Then $3^n = \frac{1}{3}$, $9^n = \frac{1}{9}$ and $\frac{1}{3} > \frac{1}{9}$, so $3^n > 9^n$, as required.

Solution to Exercise A115

There are many other possible counterexamples in each part of this exercise.

(a) Taking $m = 1$ and $n = 3$ provides a counterexample since then $m + n = 4$, which is even.

(b) The number -3 is a counterexample because $-3 < 2$ but $((-3)^2 - 2)^2 = (9 - 2)^2 = 7^2 = 49$, which is not less than 4.

(c) We look for a counterexample. Here is a table for the first few values of n .

n	1	2	3
$4^n + 1$	5	17	65

Since $4^3 + 1 = 65$ is not a prime number, it provides a counterexample, so this implication is false.

Solution to Exercise A116

The implication

$$x^2 = 9 \implies x = 3$$

is false, as $-3 \neq 3$ and $(-3)^2 = 9$, so $x = -3$ is a counterexample. Hence the equivalence is false.

Solution to Exercise A117

(a) Let $P(n)$ be the statement

$$1 + 2 + \cdots + n = \frac{1}{2}n(n+1).$$

$P(1)$ is true since $1 = \frac{1}{2}1(1+1)$.

Let $k \geq 1$, and assume that $P(k)$ is true; that is,

$$1 + 2 + \cdots + k = \frac{1}{2}k(k+1).$$

We wish to deduce that $P(k+1)$ is true; that is,

$$1 + 2 + \cdots + k + (k+1) = \frac{1}{2}(k+1)(k+2).$$

Now

$$\begin{aligned} 1 + 2 + \cdots + k + (k+1) &= \frac{1}{2}k(k+1) + (k+1) \quad (\text{by } P(k)) \\ &= (k+1) \left(\frac{1}{2}k + 1\right) \\ &= \frac{1}{2}(k+1)(k+2). \end{aligned}$$

Thus, for $k = 1, 2, \dots$,

$$P(k) \implies P(k+1).$$

Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \dots$.

(b) Let $P(n)$ be the statement

$$1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2.$$

$P(1)$ is true since

$$1^3 = 1 \quad \text{and} \quad \frac{1}{4}1^2(1+1)^2 = 1.$$

Let $k \geq 1$, and assume that $P(k)$ is true; that is,

$$1^3 + 2^3 + \cdots + k^3 = \frac{1}{4}k^2(k+1)^2.$$

We wish to deduce that $P(k+1)$ is true; that is,

$$\begin{aligned} 1^3 + 2^3 + \cdots + k^3 + (k+1)^3 &= \frac{1}{4}k^2(k+1)^2 + (k+1)^3 \\ &= \frac{1}{4}(k+1)^2(k+2)^2. \end{aligned}$$

Now

$$\begin{aligned} 1^3 + 2^3 + \cdots + k^3 + (k+1)^3 &= \frac{1}{4}k^2(k+1)^2 + (k+1)^3 \quad (\text{by } P(k)) \\ &= (k+1)^2 \left(\frac{1}{4}k^2 + (k+1)\right) \\ &= \frac{1}{4}(k+1)^2(k^2 + 4k + 4) \\ &= \frac{1}{4}(k+1)^2(k+2)^2. \end{aligned}$$

Thus, for $k = 1, 2, \dots$,

$$P(k) \implies P(k+1).$$

Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \dots$.

Solution to Exercise A118

(a) Let $P(n)$ be the statement ' $4^{2n-3} + 1$ is a multiple of 5'.

$P(2)$ is true because $4^{2 \times 2 - 3} + 1 = 4^1 + 1 = 5$.

Now let $k \geq 2$, and assume that $P(k)$ is true; that is,

$$4^{2k-3} + 1 \text{ is a multiple of 5.}$$

We wish to deduce that $P(k+1)$ is true; that is,

$$4^{2(k+1)-3} + 1 = 4^{2k-1} + 1 \text{ is a multiple of 5.}$$

Now

$$\begin{aligned} 4^{2k-1} + 1 &= 4^2 4^{2k-3} + 1 \\ &= 16 \times 4^{2k-3} + 1 \\ &= 15 \times 4^{2k-3} + 4^{2k-3} + 1. \end{aligned}$$

The first term here is a multiple of 5, and $4^{2k-3} + 1$ is a multiple of 5, by $P(k)$. Therefore $4^{2k-1} + 1$ is a multiple of 5. Hence

$$P(k) \implies P(k+1), \text{ for } k = 2, 3, \dots$$

By mathematical induction, it follows that $P(n)$ is true, for $n = 2, 3, \dots$

(b) Let $P(n)$ be the statement $5^n < n!$.

$P(12)$ is true because $5^{12} = 2.44 \times 10^8$ and $12! = 4.79 \times 10^8$, both to three significant figures.

Now let $k \geq 12$, and assume that $P(k)$ is true; that is,

$$5^k < k!.$$

We wish to deduce that $P(k+1)$ is true; that is,

$$5^{(k+1)} < (k+1)!.$$

Now

$$\begin{aligned} 5^{k+1} &= 5 \times 5^k \\ &< 5 \times k! \quad (\text{by } P(k)) \\ &< (k+1)k! \\ &= (k+1)!, \end{aligned}$$

where we have used the fact that $k \geq 12$, so $k+1 \geq 13 > 5$. Thus we have shown that

$$P(k) \implies P(k+1), \text{ for } k = 12, 13, \dots$$

Hence, by mathematical induction, $P(n)$ is true, for $n = 12, 13, \dots$

Solution to Exercise A119

Let $P(m)$ be the statement

$$\text{if } a \equiv b \pmod{n}, \text{ then } a^m \equiv b^m \pmod{n}.$$

$P(1)$ is the statement

$$\text{if } a \equiv b \pmod{n}, \text{ then } a \equiv b \pmod{n},$$

which is certainly true.

Assume that $P(k)$ is true; that is, assume that

$$\text{if } a \equiv b \pmod{n}, \text{ then } a^k \equiv b^k \pmod{n}.$$

We wish to deduce that $P(k+1)$ is true; that is,

$$\text{if } a \equiv b \pmod{n}, \text{ then } a^{k+1} \equiv b^{k+1} \pmod{n}.$$

So suppose $a \equiv b \pmod{n}$. Then, by $P(k)$, we know that $a^k \equiv b^k \pmod{n}$.

By the multiplication property of congruences, we have that

$$a^{k+1} \equiv b^{k+1} \pmod{n}.$$

Hence $P(k) \implies P(k+1)$, for $k = 1, 2, \dots$

Thus, by mathematical induction, $P(m)$ is true, for $m = 1, 2, \dots$

Solution to Exercise A120

The statement of $P(n)$ and the proof of step 1 are correct.

However, the '=' sign in the argument

$$2^k + 1 \leq 2(2^k + 1) = 2 \times 3^k \quad (\text{by } P(k))$$

is incorrect: $P(k)$ is an inequality, so we can at best conclude that $2(2^k + 1) \leq 2 \times 3^k$.

Moreover, even after replacing '=' by ' \leq ', all we can deduce is that $2^k + 1 \leq 3^{k+1}$, which is not $P(k+1)$.

A correct proof of step 2 is as follows.

Assume $P(k)$; that is, assume that $2^k + 1 \leq 3^k$. We want to deduce that $P(k+1)$ is true; that is,

$$2^{k+1} + 1 \leq 3^{k+1}.$$

Now

$$\begin{aligned}
 2^{k+1} + 1 &= 2 \times 2^k + 1 \\
 &= 2 \times (2^k + 1) - 1 \\
 &\leq 2 \times 3^k - 1 \quad (\text{by } P(k)) \\
 &\leq 3 \times 3^k - 1 \\
 &= 3^{k+1} - 1 \\
 &\leq 3^{k+1}.
 \end{aligned}$$

It follows that $2^{k+1} + 1 \leq 3^{k+1}$.

Thus $P(k) \implies P(k+1)$, for $k = 1, 2, \dots$.

Hence, by mathematical induction, $P(n)$ is true, for $n = 1, 2, \dots$.

Solution to Exercise A121

Suppose that there exists a rational number x such that $x^3 = 2$. Since x is rational, we can write $x = p/q$, where p and q are coprime positive integers.

Then the equation $x^3 = 2$ becomes

$$\left(\frac{p}{q}\right)^3 = 2,$$

that is,

$$p^3 = 2q^3,$$

which tells us that p^3 must be even. Now, the cube of an odd number, say $2k+1$ for some integer k , is odd because

$$\begin{aligned}
 (2k+1)^3 &= 8k^3 + 12k^2 + 6k + 1 \\
 &= 2(4k^3 + 6k^2 + 3k) + 1,
 \end{aligned}$$

so p must be even, and hence it can be written as $2r$ for some integer r . Then our equation becomes

$$(2r)^3 = 2q^3,$$

so we have

$$q^3 = 4r^3.$$

Hence q^3 , and therefore q , is also even, so 2 is a common factor of p and q . But p and q were assumed to be coprime, so we have obtained a contradiction.

Therefore there is no rational number x such that $x^3 = 2$.

(Alternatively, instead of proving that the cube of

an odd number is odd, you could use the fact that a positive integer is even if and only if its cube is even, which was proved in Worked Exercise A57.)

Solution to Exercise A122

(a) Suppose that there exist real numbers a and b with $ab > \frac{1}{2}(a^2 + b^2)$.

Then $a^2 - 2ab + b^2 < 0$; that is, $(a-b)^2 < 0$. Since a square can never be negative this is a contradiction, so our supposition must be false. Hence there are no such real numbers a and b .

(b) Suppose that there exist integers m and n with $5m + 15n = 357$.

Since m and n are integers, it follows that the left-hand side of this equation, $5m + 15n$, is a multiple of 5. However, the right-hand side of the equation, 357, is not a multiple of 5. This is a contradiction, so our supposition must be false. Hence there are no such integers m and n .

Solution to Exercise A123

Suppose that $n = a + 2b$, where a and b are positive real numbers. Suppose also that $a < \frac{1}{2}n$ and $b < \frac{1}{4}n$. Then

$$n = a + 2b < \frac{1}{2}n + 2\left(\frac{1}{4}n\right) = n.$$

Thus we have deduced that $n < n$. This contradiction shows that the supposition that $a < \frac{1}{2}n$ and $b < \frac{1}{4}n$ must be false; that is, we must have $a \geq \frac{1}{2}n$ or $b \geq \frac{1}{4}n$.

Solution to Exercise A124

(a) We prove the contrapositive implication, which is

$$n \text{ is even} \implies n^3 + 2n + 1 \text{ is odd.}$$

Suppose that n is even. Then $n = 2k$ for some integer k , and so

$$\begin{aligned}
 n^3 + 2n + 1 &= (2k)^3 + 2 \times 2k + 1 \\
 &= 8k^3 + 4k + 1 \\
 &= 2(4k^3 + 2k) + 1.
 \end{aligned}$$

Since $4k^3 + 2k$ is an integer, $n^3 + 2n + 1$ is odd.

Since the contrapositive is true, the original implication is also true.

(Alternatively, you may have based your proof on the fact, proved in Worked Exercise A57, that a positive integer is even if and only if its cube is even.)

(b) We prove the contrapositive implication, which is

if at least one of m and n is even, then mn is even.

Suppose that at least one of m and n is even; we can take it to be m (since otherwise we can just interchange m and n). Then $m = 2k$ for some integer k . Hence $mn = 2kn$, which is even.

(c) Let n be an integer that is greater than 1. We prove the contrapositive implication, which is

if n is not a prime number, then n is divisible by at least one of the primes less than or equal to \sqrt{n} .

Suppose that n is not a prime number. Then $n = ab$ for some integers a, b , where $1 < a, b < n$. By the result of Worked Exercise A68, at least one of a and b is less than or equal to \sqrt{n} . This number has a prime factor, which must also be less than or equal to \sqrt{n} , and this prime factor must also be a factor of n . This proves the required contrapositive implication.

Solution to Exercise A125

We prove the contrapositive implication, which is

if $A - B \neq \emptyset$, then $A \not\subseteq B$.

Suppose that $A - B \neq \emptyset$. Then there is an element x such that $x \in A$ but $x \notin B$. It follows that $A \not\subseteq B$, as required.

Solution to Exercise A126

The proof is incorrect because it has used the converse of the statement to be proved, rather than its contrapositive. The contrapositive is

if n is even, then $n^3 + 3$ is odd.

An implication and its converse are not equivalent, therefore the given argument is not a proof of the original statement. Instead, it is a correct proof by contraposition of the implication

if $n^3 + 3$ is odd, then n is even.

A correct proof of the contrapositive of the original statement is as follows. Suppose n is even. Then $n = 2k$ for some integer k , and therefore

$$\begin{aligned} n^3 + 3 &= (2k)^3 + 3 \\ &= 8k^3 + 3 \\ &= 2(4k^3 + 1) + 1. \end{aligned}$$

Since $4k^3 + 1$ is an integer, this shows that $n^3 + 3$ is odd, as required.

Solution to Exercise A127

Statement (b) is false and the other three statements are true.

Solution to Exercise A128

(a) (i) The statement $1.3 \sim 5.3$ is true because $1.3 - 5.3 = -4$ is an integer.

(ii) The statement $2.8 \sim 2.1$ is false because $2.8 - 2.1 = 0.7$ is not an integer.

(iii) The statement $2.4 \sim -5.4$ is false because $2.4 - (-5.4) = 2.4 + 5.4 = 7.8$ is not an integer.

(b) (i) A real number y such that $0.8 \sim y$ is 1.8, for example, since $0.8 - 1.8 = -1$ is an integer.

(ii) A real number z such that $0.8 \not\sim z$ is 0, for example, since $0.8 - 0 = 0.8$ is not an integer.

(There are many other possible solutions to part (b).)

Solution to Exercise A129

(a) E1 The relation 'has sat next to' is not reflexive, since no one has sat next to themselves.

E2 However, it is symmetric, because if person A has sat next to person B, then it follows that person B has sat next to person A.

(Here we have assumed that when we say 'A has sat next to B' we mean that A and B have *both* been *sitting* next to each other: we do not allow the possibility that only A sat while B stood, for example.)

E3 Finally, it is not transitive, because if person A has sat next to person B, and person B has sat next to person C, then it does not follow that person A has sat next to person C.

Hence this relation is not an equivalence relation.

(b) E1 The relation ‘was born in the same year as’ is reflexive, because each person was born in the same year as themselves.

E2 It is also symmetric, because if person A was born in the same year as person B, then it follows that person B was born in the same year as person A.

E3 Finally, it is transitive, because if person A was born in the same year as person B, and person B was born in the same year as person C, then person A was born in the same year as person C.

Hence this relation is an equivalence relation.

Solution to Exercise A130

(a) E1 Let $n \in \mathbb{Z}$. Then $n - n = 0$, which is even, so $n \sim n$. Thus \sim is reflexive.

E2 Let $m, n \in \mathbb{Z}$ and suppose that $m \sim n$. Then $m - n$ is even. Since $n - m = -(m - n)$, it follows that $n - m$ is also even. Hence $n \sim m$. Thus \sim is symmetric.

E3 Let $l, m, n \in \mathbb{Z}$ and suppose that $l \sim m$ and $m \sim n$. Then $l - m$ is even and $m - n$ is even. Since the sum of two even numbers is also even, it follows that

$$l - m + m - n = l - n$$

is also even. Hence $l \sim n$. Thus \sim is transitive.

Since \sim is reflexive, symmetric and transitive, it is an equivalence relation.

(b) E1 The relation \sim is not reflexive: for example, we have $2 \not\sim 2$, since $2 - 2 = 0$ which is not odd.

E2 Let $m, n \in \mathbb{Z}$ and suppose that $m \sim n$. Then $m - n$ is odd. Since $n - m = -(m - n)$, it follows that $n - m$ is also odd. Hence $n \sim m$. Thus \sim is symmetric.

E3 The relation \sim is not transitive: for example, $3 \sim 2$ since $3 - 2$ is odd, and $2 \sim 1$ since $2 - 1$ is odd, but $3 \not\sim 1$ since $3 - 1$ is even.

Since \sim is not reflexive (or transitive), it is not an equivalence relation.

(c) E1 Let $n \in \mathbb{Z}$. Then $n^2 + n^2 = 2n^2$, which is even since n^2 is an integer, so $n \sim n$. Thus \sim is reflexive.

E2 Let $m, n \in \mathbb{Z}$ and suppose that $m \sim n$. Then $m^2 + n^2$ is even, and so $n^2 + m^2$ is also even. Hence $n \sim m$. Thus \sim is symmetric.

E3 Let $l, m, n \in \mathbb{Z}$ and suppose that $l \sim m$ and $m \sim n$. Then $l^2 + m^2$ is even and $m^2 + n^2$ is even. Hence

$$l^2 + m^2 = 2j \quad \text{and} \quad m^2 + n^2 = 2k,$$

where $j, k \in \mathbb{Z}$. Hence

$$l^2 = 2j - m^2 \quad \text{and} \quad n^2 = 2k - m^2,$$

so

$$\begin{aligned} l^2 + n^2 &= 2j - m^2 + 2k - m^2 \\ &= 2(j + k - m^2), \end{aligned}$$

which is even, since $j + k - m^2$ is an integer. Hence $l \sim n$. Thus \sim is transitive.

Since \sim is reflexive, symmetric and transitive, it is an equivalence relation.

(d) E1 Let $z \in \mathbb{C}$. Then $|z| = |z|$, so $z \sim z$. Thus \sim is reflexive.

E2 Let $z_1, z_2 \in \mathbb{C}$ and suppose that $z_1 \sim z_2$. Then $|z_1| = |z_2|$, and so $|z_2| = |z_1|$. Hence $z_2 \sim z_1$. Thus \sim is symmetric.

E3 Let $z_1, z_2, z_3 \in \mathbb{C}$ and suppose that $z_1 \sim z_2$ and $z_2 \sim z_3$. Then $|z_1| = |z_2|$ and $|z_2| = |z_3|$. Hence $|z_1| = |z_3|$, that is, $z_1 \sim z_3$. Thus \sim is transitive.

Since \sim is reflexive, symmetric and transitive, it is an equivalence relation.

(e) E1 Let l be a line in the plane. Then l is parallel to itself, so $l \sim l$. Thus \sim is reflexive.

E2 Let l_1 and l_2 be lines in the plane and suppose that $l_1 \sim l_2$. Then l_1 is parallel to l_2 , so l_2 is parallel to l_1 . That is, $l_2 \sim l_1$. Thus \sim is symmetric.

E3 Let l_1, l_2 and l_3 be lines in the plane and suppose that $l_1 \sim l_2$ and $l_2 \sim l_3$. Then l_1 is parallel to l_2 and l_2 is parallel to l_3 . It follows that l_1 is parallel to l_3 , that is, $l_1 \sim l_3$. Thus \sim is transitive.

Since \sim is reflexive, symmetric and transitive, it is an equivalence relation.

(f) E1 Let $x \in \mathbb{R}$. Then $\lfloor x - x \rfloor = \lfloor 0 \rfloor = 0$, so $x \sim x$. Thus \sim is reflexive.

E2 The relation \sim is not symmetric: for example, $0.5 \sim 0$, since

$$\lfloor 0.5 - 0 \rfloor = \lfloor 0.5 \rfloor = 0,$$

but $0 \not\sim 0.5$, since

$$\lfloor 0 - 0.5 \rfloor = \lfloor -0.5 \rfloor = -1 \neq 0.$$

E3 The relation \sim is not transitive: for example, $1 \sim 0.5$, since

$$\lfloor 1 - 0.5 \rfloor = \lfloor 0.5 \rfloor = 0$$

and $0.5 \sim 0$, since

$$\lfloor 0.5 - 0 \rfloor = \lfloor 0.5 \rfloor = 0,$$

but $1 \not\sim 0$, since

$$\lfloor 1 - 0 \rfloor = \lfloor 1 \rfloor = 1 \neq 0.$$

Since \sim is not symmetric (or transitive), it is not an equivalence relation.

Solution to Exercise A131

(a) We start by proving properties E2 (symmetry) and E3 (transitivity) for this relation \sim , and then show that property E1 (reflexivity) does not hold.

E2 Let $x, y \in \mathbb{R}$ and suppose that $x \sim y$. Then $xy > 0$, from which it follows that $yx > 0$. Hence $y \sim x$. Thus \sim is symmetric.

E3 Let $x, y, z \in \mathbb{R}$ and suppose that $x \sim y$ and $y \sim z$. Then $xy > 0$ and $yz > 0$. By the first of these inequalities, x and y are either both positive or both negative, and by the second of the inequalities, y and z are either both positive or both negative. It follows that x , y and z are either all positive or all negative. Hence $xz > 0$. Thus \sim is transitive.

E1 The relation \sim is not reflexive; for example, $0 \not\sim 0$, because $0 \times 0 = 0$ which is not greater than 0.

(b) The error in the proof is the statement ‘Let y be an element of X such that $x \sim y$ ’. This statement makes the assumption that there is such an element y , but there may not be.

The argument in the proof is correct apart from this step, so it works for each element x that is related to another element y , but it does not work for an element x that is not related to any other

element in the set X . This is why taking \sim to be the relation defined in part (a), and taking $x = 0$, provides a counterexample: for this relation, there is no $y \in \mathbb{R}$ such that $0 \sim y$.

Solution to Exercise A132

We have

$$\begin{aligned} \llbracket 1 \rrbracket &= \{n \in \mathbb{Z} : 1 \sim n\} \\ &= \{n \in \mathbb{Z} : 1 - n \text{ is even}\} \\ &= \{n \in \mathbb{Z} : 1 - n = 2k \text{ for some integer } k\} \\ &= \{n \in \mathbb{Z} : n = -2k + 1 \text{ for some integer } k\} \\ &= \{n \in \mathbb{Z} : n = 2k + 1 \text{ for some integer } k\} \\ &= \{n \in \mathbb{Z} : n \text{ is odd}\}. \end{aligned}$$

So $\llbracket 1 \rrbracket$ is the set of odd integers.

Solution to Exercise A133

In Exercise A132 we found that $\llbracket 1 \rrbracket$ is the set of odd integers.

We might suspect that the set of even integers is also an equivalence class. To check this, we can find the equivalence class $\llbracket 0 \rrbracket$. We have

$$\begin{aligned} \llbracket 0 \rrbracket &= \{n \in \mathbb{Z} : 0 \sim n\} \\ &= \{n \in \mathbb{Z} : 0 - n \text{ is even}\} \\ &= \{n \in \mathbb{Z} : -n = 2k \text{ for some integer } k\} \\ &= \{n \in \mathbb{Z} : n = -2k \text{ for some integer } k\} \\ &= \{n \in \mathbb{Z} : n \text{ is even}\}. \end{aligned}$$

So, as suspected, $\llbracket 0 \rrbracket$ is the set of even integers.

Since the set of even integers and the set of odd integers form a partition of the set \mathbb{Z} , they are the only two equivalence classes of \sim .

Solution to Exercise A134

(a) E1 Let $x \in \mathbb{R}$. Then $\lfloor x \rfloor = \lfloor x \rfloor$, so $x \sim x$. Thus \sim is reflexive.

E2 Let $x, y \in \mathbb{R}$ and suppose that $x \sim y$. Then $\lfloor x \rfloor = \lfloor y \rfloor$, that is, $\lfloor y \rfloor = \lfloor x \rfloor$. Hence $y \sim x$. Thus \sim is symmetric.

E3 Let $x, y, z \in \mathbb{R}$ and suppose that $x \sim y$ and $y \sim z$. Then $\lfloor x \rfloor = \lfloor y \rfloor$ and $\lfloor y \rfloor = \lfloor z \rfloor$. Hence $\lfloor x \rfloor = \lfloor z \rfloor$, that is, $x \sim z$. Thus \sim is transitive.

Since \sim is reflexive, symmetric and transitive, it is an equivalence relation.

(b) We have

$$\begin{aligned}
 \llbracket 1 \rrbracket &= \{y \in \mathbb{R} : 1 \sim y\} \\
 &= \{y \in \mathbb{R} : \lfloor 1 \rfloor = \lfloor y \rfloor\} \\
 &= \{y \in \mathbb{R} : 1 = \lfloor y \rfloor\} \\
 &= \{y \in \mathbb{R} : \lfloor y \rfloor = 1\} \\
 &= [1, 2).
 \end{aligned}$$

That is, the equivalence class $\llbracket 1 \rrbracket$ is the interval $[1, 2)$.

Similarly, we have

$$\begin{aligned}
 \llbracket -4 \rrbracket &= \{y \in \mathbb{R} : -4 \sim y\} \\
 &= \{y \in \mathbb{R} : \lfloor -4 \rfloor = \lfloor y \rfloor\} \\
 &= \{y \in \mathbb{R} : -4 = \lfloor y \rfloor\} \\
 &= \{y \in \mathbb{R} : \lfloor y \rfloor = -4\} \\
 &= [-4, -3).
 \end{aligned}$$

That is, the equivalence class $\llbracket -4 \rrbracket$ is the interval $[-4, -3)$.

(c) The equivalence classes of \sim are the intervals of the form $[n, n+1)$ where n is an integer. The collection of all such intervals partitions the set \mathbb{R} .

Solution to Exercise A135

E1 Let $x \in X$. Then x belongs to the same subset in the partition as itself, so $x \sim x$. Thus \sim is reflexive.

E2 Let $x, y \in X$ and suppose that $x \sim y$. Then x and y belong to the same subset in the partition, so $y \sim x$. Thus \sim is symmetric.

E3 Let $x, y, z \in X$ and suppose that $x \sim y$ and $y \sim z$. Then x and y belong to the same subset in the partition, and y and z belong to the same subset in the partition. It follows that x, y and z all belong to the same subset in the partition, so $x \sim z$. Thus \sim is transitive.

Since \sim is reflexive, symmetric and transitive, it is an equivalence relation.

Solution to Exercise A136

Since $4 + 4 = 8$ and the equivalence class $\llbracket 8 \rrbracket$ of congruence modulo 5 contains the element 3 of \mathbb{Z}_5 , we have $4 +_5 4 = 3$.

Similarly, since $3 \times 4 = 12$ and the equivalence class $\llbracket 12 \rrbracket$ of congruence modulo 5 contains the

element 2 of \mathbb{Z}_5 , we have $3 \times_5 4 = 2$.

Solution to Exercise A137

(a) The solution to Exercise A133 shows that \sim has only two equivalence classes, namely the set of all even integers and the set of all odd integers.

So a suitable set of representatives is the set $\{0, 1\}$.

(There are other choices, of course: any set containing exactly one even integer and exactly one odd integer, such as $\{22, 7\}$ or $\{4, -1\}$, is a set of representatives, but $\{0, 1\}$ (that is, \mathbb{Z}_2) is the most natural choice.)

(b) In Exercise A134 it was found that the equivalence classes of \sim are the intervals of the form $[n, n+1)$ where n is an integer.

A suitable set of representatives is \mathbb{Z} .

(There are other choices, such as the set $\{n + \frac{1}{2} : n \in \mathbb{Z}\}$, but \mathbb{Z} is the most natural choice.)